NOVELL®

NetWare Version 2.2

Concepts

NetWare®

NOVELL®

NetWare Version 2.2

Concepts

NetWare®

Disclaimer

Novell, Inc. makes no representations or warranties with respect to the contents or use of this manual, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any NetWare software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of NetWare software, at any time, without obligation to notify any person or entity of such changes.

Copyright

© Copyright 1983-1991 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express prior written consent of the publisher.

Novell, Inc.
122 East 1700 South
Provo, Utah 84606 USA

March 1991 Edition
For NetWare v2.2
Novell Part # 100-000895-001

HRT .::::: 91

65910

How to use this manual

This manual is designed to be used as an extended glossary of NetWare-related terms.

Use *Concepts* as a reference if you have questions as you complete network installation or maintenance.

Entries are arranged alphabetically; the beginning of each alphabetical section is clearly marked (**AAA**, **BBB**, etc.).

This manual contains three types of cross references:

- **To other entries in *Concepts*.** These appear in boldface. If a concept is not explained completely in one part of the manual, you are referred by a "See" or a "See also" reference to the entry in which that concept is explained in detail. For example, the entry **Account, user** refers you to **User account**. Go to **User account** for a complete explanation.
- **To related utilities.** Utility names appear in full capitals. For example, the entry **File server console operator** contains an explanation and then refers you to related utilities, FCONSOLE and SYSCON, in *Using the Network*. Refer to the "Utilities" section of *Using the Network* for additional information.
- **To sections of other manuals.** Manual sections are enclosed in quotation marks; manual titles appear in italic font. Use the table of contents in each manual to locate the information you need.

Consult the Master Index to locate instructions and additional information in other manuals.

User comments

We are continually looking for ways to make our products and our manuals as easy to use as possible. You can help us by sharing your comments and suggestions about our manuals. Tell us how we can make them more useful to you and point out any inaccuracies or information gaps they contain.

Use the "User comments" form at the end of this manual to submit your comments or write to us directly at the following address:

Novell, Inc.
Technical Publications
122 East 1700 South MS C-24-1
Provo, UT 84606 USA

We sincerely appreciate your comments about our products.

AAA

Abend (Abnormal end)

When the operating system detects a serious problem, such as a hardware or software failure, the system issues an abend (abnormal end) message. The abend stops the file server.

See "Abend" in the Master Index.

Access control right

See **Security (Rights security).**

Access privileges

See **Security (Rights security).**

Account, user

See **User account.**

Account restrictions

See **Security.**

Accounting

The accounting option allows network supervisors to

- Charge users for file server resources
- Monitor file server usage

Using the "Accounting" option in SYSCON, the supervisor can

- Install accounting on a file server (accounting cannot be activated until after the file server has been installed)
- Select the services to be charged for
- Determine the amount to be charged for each service

Account balances. The network supervisor can do the following:

- Assign an individual user an account balance that determines how much of a given service the user can use.
- Assign a credit limit that the user can draw upon (or allow unlimited credit).
- Assign a system or default account balance that is assigned automatically to any user created after the default is set.
- Increase a user's account balance. The user must log out and log in again before changes will take effect.

The supervisor should carefully monitor account balances. Users need to know that they should respond immediately if they receive a message to log out because their account balances are too low.

If users do not log out, the file server will automatically log them out. Any data that has not been saved will be lost. Users must then have the supervisor increase their balance.

Accounting options. Once the network supervisor has installed accounting, NetWare tracks user logins and logouts automatically and stores the information in the NET$ACCT.DAT file in the SYS:SYSTEM directory. (The file server does not charge for tracking logins and logouts.)

The supervisor can choose to charge each user's account for one or more of the following services or resources:

- **Blocks Read** sets up charge rates for the amount of data read from the server. The network supervisor specifies the amount charged per block read and may vary the rate based on the time of day, modifiable in half-hour increments. (One block is 4KB.)
- **Blocks Written** sets up charge rates for the amount of data written to the file server disk(s). The supervisor specifies the amount charged per block written and may vary the rate based on the time of day, modifiable in half-hour increments.
- **Connect Time** sets up charge rates for the amount of time a user is logged in to a server. The supervisor specifies the amount charged per minute and may vary the rate based on the time of day, modifiable in half-hour increments.
- **Disk Storage** sets up charge rates for the amount of data stored on the file server disk(s). The supervisor specifies the amount charged per block per day and may vary the rate based on the time of day, modifiable in half-hour increments. We recommend specifying a special time of the day to charge for blocks in disk storage, such as 6 pm, after most users have completed their day's work. Do this by specifying a charge rate for the half-hour increment at 6 pm.

- **Service Requests** sets up charge rates for the amount of any request for service from the file server, such as listing the files in a directory. The supervisor specifies the amount charged per request received and may vary the rate based on the time of day.

If the supervisor installs accounting but chooses not to charge for services, user logins and logouts will still be tracked. (Use ATOTAL to summarize services used and PAUDIT to view accounting records.)

Accounting servers. When the network supervisor sets up accounting in SYSCON, the current file server automatically begins to charge for services. The supervisor can authorize other network servers (print servers, database servers, or gateways) to charge for services, or can revoke a server's right to charge.

Add accounting servers. The network supervisor decides which servers have the right to track and charge users. Adding the server to the "Accounting servers" list in SYSCON automatically authorizes the server to charge for services.

Delete accounting servers. Delete the server from the "Accounting Servers" list.

Charge rates. Before setting charge rates for services, the supervisor should do the following:

- Determine what services to charge for and the return that needs to be realized for each service.

  For example, if file server storage capacity is a concern, the supervisor might charge for disk storage. If network utilization is high, the supervisor might charge for service requests. If users should not be logged in when they are not working, the supervisor might charge for connect time.

- Determine the cost of a service and the amount to charge over a given period of time.

- Use ATOTAL to monitor the file server for two or three weeks. ATOTAL tracks daily and weekly use of each service. At the end of the monitoring period, determine the percentage of use for each service. (ATOTAL is run from the SYS:SYSTEM directory, which requires supervisor rights.)

  If, for example, 30% of the file server's charges stem from service requests, you would want to recoup 30% of operating costs by charging for service requests.

Calculate charge rates on the basis of one charge per unit of the specified service. The unit of charge is arbitrary, but we suggest that the supervisor begin with 1 charge unit equaling 1¢. Adjust this ratio if it does not work for your network environment.

Charge rates are specified as ratios as in the formula below:

$$\frac{\text{Charge (charge rate multiplier)}}{\text{Estimated usage (charge rate divisor)}} = \text{Total charge}$$

For example, if you need to charge $100 a month for blocks read to cover costs and you know that 250,000 blocks are read each month, the charge rate would be $100 divided by 250,000 blocks, or 4¢ a block.

See "Managing accounting" in *Using the Network* for additional examples.

Remove accounting. To deactivate accounting and remove it from the file server, delete all accounting servers and then remove the accounting feature.

Related utilities: ATOTAL, PAUDIT, SYSCON (see *Using the Network*).

Active hub

A device used to amplify transmission signals in certain network topologies. You can use an active hub to add workstations to a network or to lengthen the cable distance between workstations and the file server.

See also **Passive hub.**

Add-on board

An optional circuit board that modifies or enhances a personal computer's capabilities.

See also **Memory board; Network board.**

Address

See **Configuration option; Controller address; Network addresses; Node number; SCSI bus.**

Application

A software program or program package that makes calls to the operating system and manipulates data files, thus allowing a user to perform a specific job (such as accounting or word processing). An application is a tool for performing a task.

Standalone application. An application that runs from the hard disk or floppy disks in a self-contained, independent computer. Only one user can access the application at a time.

Network application. An application that runs on networked computers and can be shared by a number of users. Lock-out, file attributes, and trustee rights are needed for network security purposes. Network applications use network resources such as printers. Advanced network applications (such as electronic mail) allow communication among users.

Archive Needed attribute

See **Security (Attribute security).**

Asynchronous transmission

See **Serial communication.**

ATTACH

Command that assigns a connection number to a workstation and attaches the workstation to the LOGIN directory on the default (or specified) file server. As many as 100 workstations can be attached to a file server running NetWare v2.2.

When loaded, the NetWare shell (workstation file NET*x*.COM) automatically attaches your workstation to the nearest file server. You can also specify in SHELL.CFG which server you prefer to attach to.

See also **NetWare workstation files;** "Managing DOS workstations" in *Using the Network.*

Attributes

See **Security.**

AUTOEXEC.BAT

See **Boot files.**

AUTOEXEC.SYS

See **Boot files.**

Automatic rollback

A feature of the Transaction Tracking System (TTS) that returns a database to its original state. When a network running under TTS fails during a transaction, the database is "rolled back" to its most recent complete state, preventing corruption from the incomplete transaction.

BBB

Backing out

See **TTS.**

Backup

A stored copy of a file, directory, or volume preserved as a safeguard in case the original is corrupted or destroyed.

Current and valid backups are essential for smooth maintenance. Every administrator, sooner or later, experiences a hardware or software failure that requires the restoration of data from a backup.

A network includes setup information (such as users, directories, login scripts, rights, drive mappings, passwords, and batch files) that is difficult to recreate. To avoid having to repeat the complete setup if the file server crashes or you lose data, you must occasionally back up the complete network.

A complete network setup includes a careful scheme for backing up and archiving data so it is always accessible. Since you want to protect your data in every way you can, invest in a good backup device and back up your file server regularly.

Types of backups. There are two main types of backups:

- **Complete** backups include all files on a disk. This type of backup is time consuming, but all the files are copied.
- **Partial** backups include only specified files, usually those that have been modified since the last backup. Most backup media allow you to specify which files to back up by specifying specific files and directories or by specifying files by dates or other characteristics. Partial backups are usually performed more frequently and can be used to supplement the last complete backup.

We recommend keeping at least two sets of storage media for backups, one set for the current backup and the other to store a previous backup.

We recommend keeping copies of your backup media (tapes or floppies) in a safe, off-site storage site so that data can be restored if your building and computer system are damaged or destroyed or on-site copies are stolen.

When to back up. Only you can determine how frequently you need to back up your system. A good rule of thumb is to consider how much money and time you would lose if you lost everything on the file server and then plan your backup schedule accordingly.

We recommend backing up your files in at least the following situations:

- On a regular weekly basis. To save time, you may want to do a partial backup daily and a complete backup only once a week. Then, if you need to restore the complete system, restore the complete backup first; then restore each subsequent partial backup, oldest first.
- Before you run any network repair utility, such as VREPAIR.
- Whenever you update your network (add a bridge or a hard disk or modify volume information, for example).

In addition, encourage network users to back up their own work whenever it changes significantly. They can copy essential files to floppy diskettes or to a hard disk, or they can use NBACKUP to back up their files.

We also recommend making TWO backup copies of your entire network, including the bindery. If you use the NetWare NBACKUP utility, the entire network structure (including hidden and system files that you can't access or modify) is backed up.

After you complete a backup, test your backup by renaming a few files and then restoring their counterparts from the backup files. Create a few "dummy" files for this purpose instead of using valuable files.

Base I/O address

See **Configuration option.**

Base memory address

See **Configuration option.**

Baud rate

See **Printing; Serial communication.**

Bindery

Network database containing definitions for entities such as users, groups, and workgroups. The bindery contains three components: objects, properties, and property data sets.

Objects represent any physical or logical entity, including users, user groups, file servers, print servers, or any other entity given a name.

Properties are the characteristics of each bindery object, including passwords, account restrictions, account balances, internetwork addresses, lists of authorized clients, workgroups, and group members.

Property data sets are values assigned to entities' bindery properties.

The NetWare v2.2 bindery consists of two hidden files located in the SYS:SYSTEM directory: NET$BIND.SYS (for objects and properties), and NET$BVAL.SYS (for property data sets).

Example. When user LYNN logs in to a file server, LOGIN checks NET$BIND.SYS for a valid object LYNN. If it exists, LOGIN reads the properties associated with that object (in this case, since LYNN is a user, LOGIN checks for a password property). If object LYNN has a password property, LOGIN prompts for the password and compares the password that is entered (a value) with the value (property data set) in NET$BVAL.SYS that is assigned to the password property. If the two values match, LYNN is logged in and allowed to use that network's resources in accordance with other values assigned to his account: account restrictions, trustee rights, etc.

See also **Security (Login security, Rights security).**

BIOS (Basic Input/Output System)

A set of programs, usually in firmware, that enables each computer's central processing unit to communicate with printers, disks, keyboards, consoles, and other attached input and output devices.

Block

A unit of stored data. In NetWare, a block is 4KB (4,096 bytes) of data. For example, a 40MB hard disk contains roughly 10,000 blocks of data storage area.

Board

See **Network board; Controller.**

Boot files

Boot files are executable programs that load an operating system and tailor your environment. This entry explains NetWare-specific boot file information and how files affect network station environment.

We recommend making a **master workstation diskette** for each unique combination of workstation boot files required by the workstations on your network.

If every workstation is the same brand, uses the same network board set to the same configuration option, and boots with the same version of DOS, you need to make only one master diskette.

DOS workstation boot files. A DOS workstation on a NetWare network boots just like a standalone computer. NetWare's only requirement is that you add two lines in the CONFIG.SYS file to set the open files and buffers above the default.

```
buffers=20
files=20
```

After the workstation boots DOS, you must enter commands at the command line to make a connection with the network. The commands you enter depend on the version of DOS the workstation is running, the type of network workstation files you are loading, and whether your workstation contains hardware that requires additional files.

We recommend putting the required commands in an AUTOEXEC.BAT file instead of entering them separately.

AUTOEXEC.BAT. You can do the following tasks through a batch file:

- Load the NetWare workstation files.
- Run additional files required by the hardware.
- Set the DOS prompt to show the directory path—a commonly used command is `prompt $p$g`.
- Change the prompt to the first network drive—usually drive F.
- Log in to a file server.

Which workstation files are required? After the DOS command line appears, you must run two files to connect to the network: IPX.COM and NET*x*.COM.

- IPX.COM is a communication protocol file configured by WSGEN for the network board installed in the workstation.
- NET*x*.COM (or EMSNET*x*.EXE or XMSNET*x*.EXE) is a shell file that corresponds to the version of DOS running on the workstation. For example, NET3.COM is used with DOS v3.*x*.

The following charts illustrate the variety of NetWare workstation files.

Required NetWare workstation files (2)	Function
IPX.COM	Interface file linked and configured with WSGEN that supplies the IPX/SPX (**I**nternetwork **P**acket e**X**change / **S**equenced **P**acket e**X**change) protocol
and	
NETx.COM	NetWare shell file corresponding to the DOS version used
or	
EMSNETx.EXE	NetWare Expanded Memory shell file corresponding to the DOS version used (LIM 4.0 EMS compatible)
or	
XMSNETx.EXE	NetWare Extended Memory shell file corresponding to the DOS version used (XMS 2.0 compatible)

Optional NetWare workstation files	Function
NETBIOS.EXE	NetWare NetBIOS emulator program that allows workstations to run applications written for peer-to-peer communication or distributed processing
and	
INT2F.COM	NetWare program that should be used with the NetBIOS emulator program
ROUTE.COM	NetWare program for workstations on a Token-Ring network with IBM bridges

If you boot the workstation from floppy diskette, copy the necessary files to a formatted boot diskette. If you boot from a hard disk (with system files and active partition), copy the files to the root directory (C:\) or a subdirectory where AUTOEXEC.BAT runs them.

Note: If you are using the extended or expanded memory shell, copy the .SYS files from the memory application's diskettes. Specify these files as device drivers in your CONFIG.SYS file so that they will load when the workstation boots. For example, add the line: `device=himem.sys`.

ODI (Open Data-Link Interface) workstation boot files. ODI drivers allow communication in NetWare and other networking environments by supporting multiple protocols and drivers. ODI is useful if you are using third-party LAN drivers written to ODI specifications or if you want to free up memory by using only the portions of IPX/SPX and diagnostics that you need.

Four files allow ODI workstations to "talk" to each other, to the file server, and to other third-party hosts.

- The link support layer file, LSL.COM, enables the workstation to communicate over several protocols.
- The LAN driver file, such as NE2000.COM or NE2.COM, provides communication between the link support layer and the network board.
- The protocol stack file, such as IPXODI.COM for NetWare networks, manages communications among the network stations.
- The NetWare workstation shell file, NET*x*.COM, redirects messages from DOS to the network.

Note: If you are using remote boot, you will need to run RPLODI.COM after you run LSL.COM and before you load your LAN driver file.

If you are using IBM Token-Ring or IBM PCnet networks, you must use additional files. See your IBM Token-Ring or IBM PCnet manual for details.

See also **ODI.**

SHELL.CFG. The SHELL.CFG file is a specialized text file created with any ASCII text editor and included with other necessary boot files. Similar to the DOS CONFIG.SYS file, the SHELL.CFG file contains configuration values that are read and interpreted when your workstation attaches to the network. These values adjust the operating parameters of the NetWare shell, IPX, or NETBIOS.

SHELL.CFG configures the NetWare shell (NET*x*.COM). Because the shell is responsible for many routines and processes in a network workstation, you might want to change the values of certain shell parameters to modify the shell's reaction to those routines and processes.

You can customize certain functions of the NetWare workstation files, such as the search mode used by the shell. If you are using any non-IBM workstations on your network, use the SHELL.CFG file to set the long machine name to allow NetWare to find the correct version of DOS on the network. See **Long machine type** for details.

Databases, multitasking, or NetBIOS applications (involved in peer-to-peer communications or distributed processing) may require parameter values different from the default values to function properly on the network. To find out which parameters you might need to modify, consult the setup documentation for each application used on your network. You might also find that you can solve printing, file retrieval, and other network problems by adjusting shell parameters.

Note: Your workstation can hang if you press the <Shift> <PrintScreen> keys on your keyboard when none of your LPT ports are captured and no local printers are attached to your workstation. To prevent this, include the following in your SHELL.CFG file on your workstation boot diskette: `local printers=0`.

The workstation will try to find a local port and quickly free itself.

For instructions on creating a SHELL.CFG file and modifying various parameters, see "Managing DOS workstations" in *Using the Network*.

NET.CFG. Like SHELL.CFG, NET.CFG contains configuration information for the workstation and is an ASCII text file created with any DOS text editor. NET.CFG was developed to enable more versatility with ODI workstations and requires v2.2 shells.

An ODI workstation may require NET.CFG along with SHELL.CFG. In most situations, you do not need NET.CFG because the established defaults are adequate.

Dedicated file server boot files. Dedicated file servers boot from floppy diskette or hard disk.

Floppy diskette. The floppy diskette boot process loads DOS, and then runs NET$OS.EXE to bring up the file server. You can use AUTOEXEC.BAT to run NET$OS.EXE. Dedicated NetWare file servers take over complete operation of the computer from DOS.

Hard disk. A PC's ROM-BIOS reads track 0 of the hard disk and finds the NetWare cold boot loader. This file automatically runs NET$OS.EXE to load the NetWare operating system.

See also "File server definition" in *Installing and Maintaining the Network*.

SERVER.CFG. The SERVER.CFG file is a NetWare file server configuration file. It is created with any text editor and is placed in the SYS:SYSTEM directory; it contains information that allows the server to

- Back out transactional files (the transactional attribute has been set) automatically
- Run VAPs automatically
- Work with UPS monitoring hardware

AUTOEXEC.SYS. The AUTOEXEC.SYS file is created using SYSCON and is stored in the SYS:SYSTEM directory. It contains console commands you want executed each time the file server comes up, such as printer setup commands.

See also **Printing (Printing files).**

Nondedicated file server boot files. Nondedicated file servers must first boot DOS from floppy diskette or hard disk. After you load NET$OS.EXE, the DOS prompt appears. We recommend that you use AUTOEXEC.BAT to load NET*x*.COM, change to drive F, and log in.

Note: IPX.COM is coded into the NetWare nondedicated operating system for file servers and routers. The workstation on a nondedicated server or router needs to load only NET*x*.COM before logging in from drive F. Then use CONSOLE.COM in SYS:LOGIN to switch from DOS to the file server console. Use DOS (also coded into the nondedicated operating system) to switch back.

Floppy diskette. The floppy diskette boot process loads DOS and then runs NET$OS.EXE to bring up the file server. You can use AUTOEXEC.BAT to run NET$OS.EXE and NET*x*.COM, change to drive F, and log in to the file server as a workstation.

Hard disk. You must include a DOS partition and make it active in order for a nondedicated file server to boot from the first hard disk. You can use AUTOEXEC.BAT to run NET$OS.EXE and NET*x*.COM, change to drive F, and log in to the file server as a workstation.

See also "File server definition" in *Installing and Maintaining the Network*.

SERVER.CFG and AUTOEXEC.SYS. These files remain the same as those for dedicated file servers. See the explanations above.

Router boot files. Whether you boot a dedicated or nondedicated router, you may want to automate the boot process in AUTOEXEC.BAT.

Dedicated routers generally boot from floppy diskette because a hard disk in a dedicated router cannot be used while the router is running. Boot with DOS and then run ROUTER.EXE to bring up the router.

Nondedicated routers. To boot a nondedicated router from hard or floppy diskette, boot with DOS and then run ROUTER.EXE and NET*x*.COM; change to drive F and log in to a file server as a workstation.

ROUTER.CFG. The ROUTER.CFG file is a NetWare router configuration file containing information to automatically run VAPs. You create it with any text editor and place it in the same directory as the ROUTER.EXE you use to bring up the router.

See also **Router**; "Managing Routers" in *Using the Network*.

Boot record

The boot record contains information that ROM-BIOS uses to determine which device to boot from. The boot record can be on either a floppy diskette or a local hard disk. ROM-BIOS then runs a short program from the boot record to determine disk format and the location of system files and directories. Using this information, ROM-BIOS loads the system files (including two hidden files, IBMBIO.COM and IBMDOS.COM) and the command processor (COMMAND.COM).

BOOTCONF.SYS

See **Remote boot (BOOTCONF.SYS).**

Bridge

See **Router.**

Buffer

An area in the file server's memory set aside to temporarily hold data.

See **Cache buffer; Communication buffer.**

Bus

A signal route for transmitting data between parts of the network. Several devices can be connected to a single bus, allowing them to share the same data pathway.

Data bus is the primary bus inside a personal computer.

Network bus is the main network cable or line that connects network stations.

CCC

Cabling system

See **Topology.**

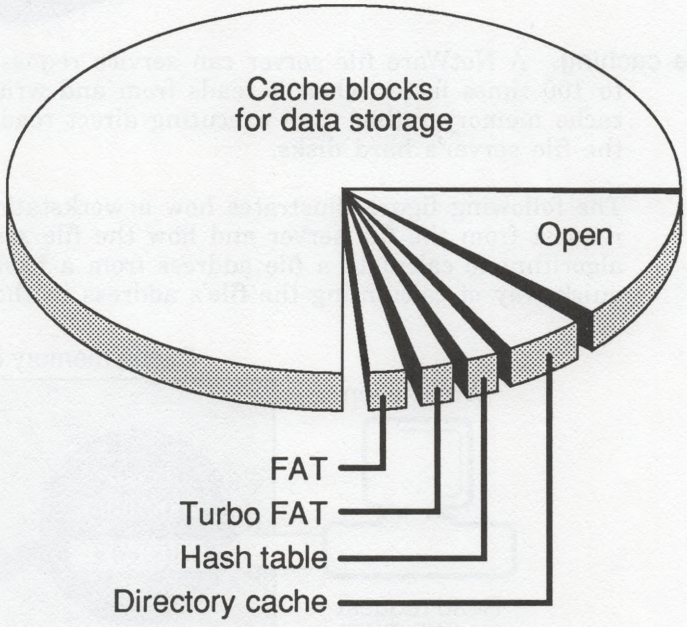
Cache buffer

A block (4KB) of file server cache memory.

See also **Cache memory.**

Cache memory

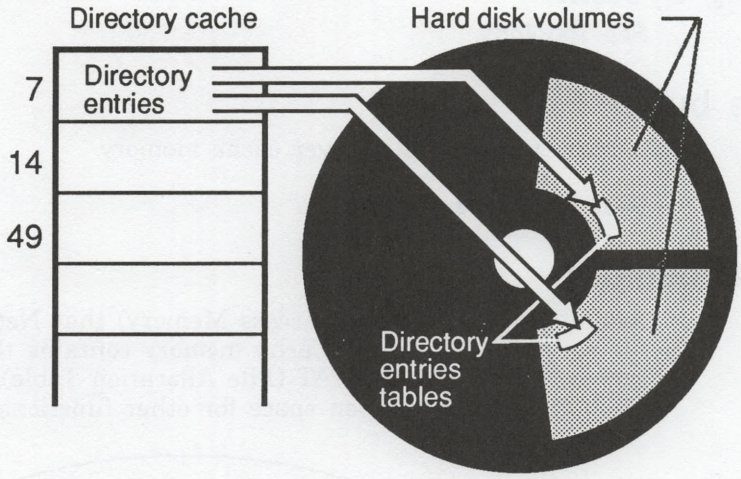
Available RAM (Random Access Memory) that NetWare uses to improve file server access time. Cache memory contains the directory and file caches, along with the FAT (File Allocation Table), the turbo FAT, the Hash table, and an open space for other functions.



Cache memory in file server RAM

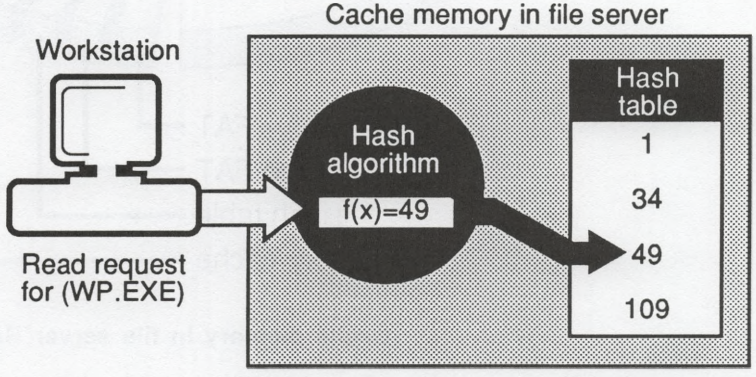
A file takes the same number of blocks (4KB) in cache memory as on a file server hard disk.

Directory caching. A method of decreasing the time it takes to determine a file's location on a disk. The FAT and directory entry table are written into the file server's memory. The area holding all directory entries is called the directory cache. The file server can find a file's address (from the directory cache) and the file data (from the file cache) much faster than retrieving the information from disk.

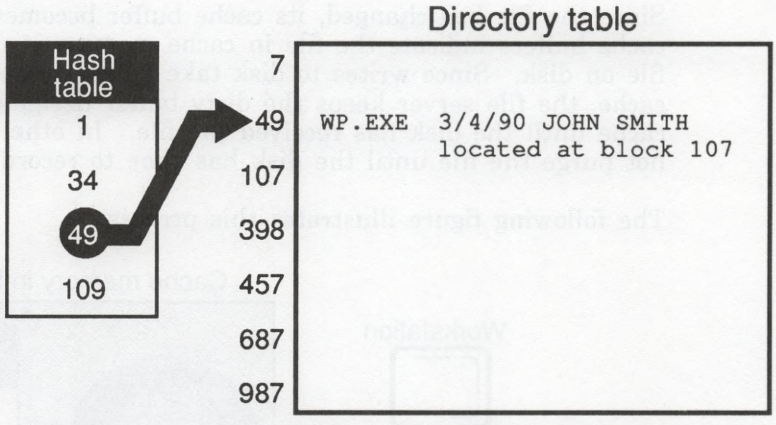


File caching. A NetWare file server can service requests from workstations up to 100 times faster when it reads from and writes to the file server's cache memory rather than executing direct reads from and writes to the file server's hard disks.

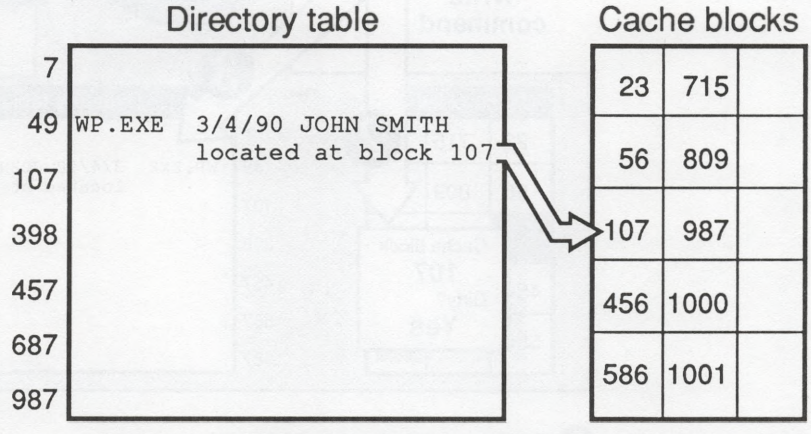
The following figure illustrates how a workstation makes a read request from the file server and how the file server executes a hash algorithm to calculate a file address from a hash table. Hashing is a quick way of calculating the file's address in the directory table.



For example, the address on the Hash table contains pointers to the first and second probable locations of the WP.EXE file's directory entry in the directory cache. If the first search is not successful, the file server uses the second pointer to find the directory entry, as in the following figure.



After the entry is located, the file server checks its cache memory to see if it contains a copy of the WP.EXE file, as in the following figure.

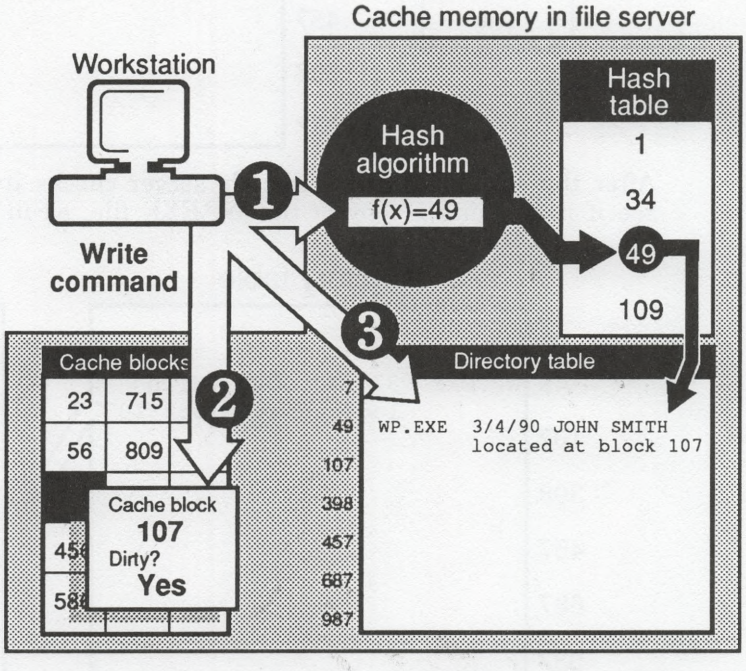


If the file is there, the server sends the file to the workstation directly from cache memory. If the file is not there, the file server retrieves the file from the hard disk, places it in cache memory, and sends it to the workstation.

Writing files to cache. When a workstation writes a file to the file server, the file server performs the hash algorithm to find the file's cache buffer. It writes the file to the designated location (writing over the old file, if the file was already in cache) and then updates the directory table in the directory cache.

Since the file has changed, its cache buffer becomes "dirty." Dirty cache buffers indicate the file in cache memory is different from the file on disk. Since writes to disk take longer to perform than writes to cache, the file server keeps the dirty buffer designation on the file in cache until the disk has received the file. In other words, RAM will not purge the file until the disk has time to record it correctly.

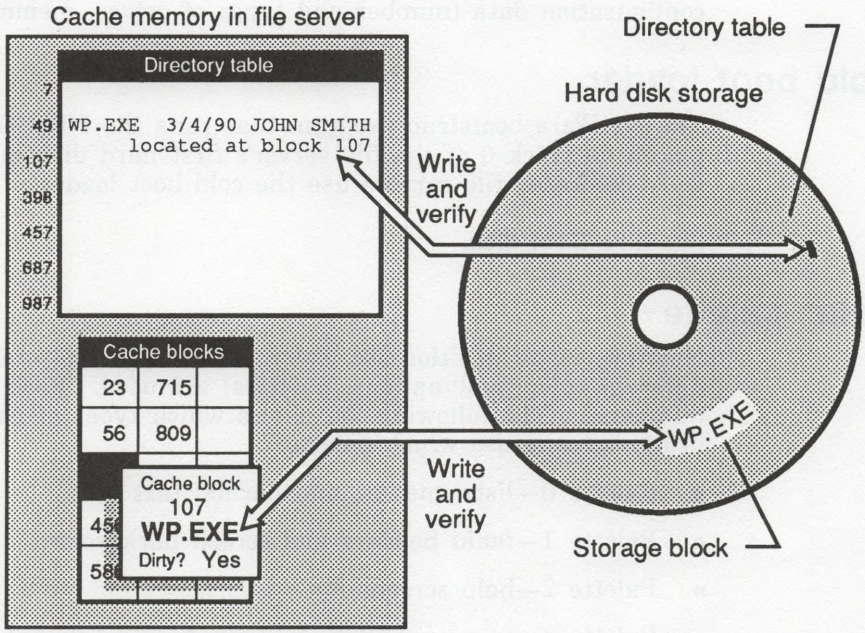
The following figure illustrates this process.



The file server sends a message to the workstation that the file server has received the file, and the workstation is free to complete other processes. Once the file is written to disk, the file server checks the data in memory against the data on disk.

If the data in memory and on disk match, the buffer is no longer dirty. As the cache memory fills up, buffers containing least used files and directories are eliminated.

The following figure illustrates the write and verify process between cache memory and hard disk storage.



See also **Data protection; Directory entry; FAT.**

Channel

The logical location of hard disk controller hardware for the flow of data. For instance, a hard disk controller in a PC is installed in a channel, or an HBA and its disk subsystems make up a disk channel. Available channels normally include 0 through 4. Channel 0 is normally used by internal controllers and hard disks.

See also **Configuration option.**

Character length

See **Serial communication.**

Charge rates

See **Accounting.**

CMOS RAM

Battery-maintained random access memory for storing system configuration data (number and types of drives, memory amount, etc.).

Cold boot loader

The NetWare bootstrap program that runs the NET$OS.EXE file. It is placed on track 0 of the file server's first hard disk during installation. Only dedicated file servers use the cold boot loader.

See also **Boot files.**

Color palette

NetWare menu utilities use "color palettes" to set screen colors. Five different color combinations (palettes) are used. Each palette is numbered. The following list shows which types of NetWare menu utility screens use which palette.

- Palette 0—lists, menus, and normal text
- Palette 1—main headers and screen background
- Palette 2—help screens
- Palette 3—error messages
- Palette 4—exit and alert portals

Overlay files. Color palette definitions are stored in special overlay files. Two pre-defined color palette files, loaded into SYS:PUBLIC, are supplied with NetWare:

- IBM$RUN.OVL—specifies color combinations for five default palettes.
- CMPQ$RUN.OVL—specifies black and white combinations for five default palettes.

Some monitors, such as monochrome monitors using composite color adapters, display unreadable screens if the first overlay file is used. Novell developed the second overlay file to solve this problem.

Overlay files and short machine type. Which overlay file you use depends on the short machine type set for the workstation in the SHELL.CFG file.

If a short machine type is not set, NetWare assumes the default, IBM, and uses the IBM$RUN.OVL overlay file. This file specifies white letters and blue background for color palette 0, cyan letters and blue background for color palette 1, and so on.

You can ensure proper screen resolution on workstation monitors by specifying an overlay file and a matching short machine type for each workstation type. For example, if you have AT&T workstations that need to use the black and white overlay file, you could set the short machine type in SHELL.CFG to "AT&T," and then copy or rename CMPQ$RUN.OVL to AT&T$RUN.OVL in SYS:PUBLIC. All workstations of the AT&T short machine type would then use the AT&T overlay file for NetWare menu utilities.

See also **Short machine type.**

Overlay file search. The shell searches for the proper overlay file each time a workstation runs a NetWare menu utility. Since the first search drive is usually mapped to SYS:PUBLIC, the shell uses the overlay file in that directory. However, if a copy of the specified overlay file is found in the default directory or in another drive that is searched before SYS:PUBLIC, that file will be used.

COLORPAL and MENU. Users can modify color palettes using COLORPAL.

Supervisors, or anyone with Read, File scan, Write, and Erase trustee rights in SYS:PUBLIC, can modify the system color palettes by running COLORPAL from SYS:PUBLIC.

Other network users can create customized color palettes in another directory (such as their home directory) in which they have Create, Write, and Erase rights. By running COLORPAL from that directory, they create a new overlay file. Users must then ensure that the shell finds the customized overlay file first, either by running menu utilities from the directory containing the newly created file, or by mapping their first search drive to the directory using MAP INS S1:=*directoryname*.

COLORPAL also allows users to specify new palettes for menus created with MENU.

Note: Modification of the default color palettes (0 through 4), which are used by NetWare utilities, is discouraged. Although color manipulation is easy, changes to the default are difficult to keep track of and sometimes result in hard-to-read screens. If you want to use different color palettes for menus you create, insert and create new palettes (5 and up) for MENU instead of modifying the default palettes.

Related utilities: COLORPAL; MENU (see *Using the Network*).

COM1, COM2

See **Serial port.**

Command format

A pattern that shows the proper way to enter a command at the computer keyboard. In NetWare manuals, a command format may include constants (+,-), variables (names), and symbols (*.*).

Communication

See **Network communication; Serial communication.**

Communication buffer

An area in the file server's memory set aside to temporarily hold data "packets" arriving from the various network stations. The packets remain in this buffer until the file server is ready to process them and send them to their destination on the network. This ensures the smooth flow of data into the file server, even during times of particularly heavy input/output operations.

The default number of communication buffers is set to 150. INSTALL will allow you to change the default setting from 40 to 1000 buffers, but since communication buffers take very little memory, we recommend you use the default or higher.

If the set maximum number of communication buffers is reached and a new packet arrives, the operating system discards the packet and the station must resend it. This should happen rarely, if ever. If the Statistics Summary in FCONSOLE indicates that the Peak Used number is frequently close or equal to the Maximum number received, increase the number of communication buffers.

Communication protocols

A set of conventions or rules used by a program or operating system to establish communication between two or more endpoints. Many different types of communication protocols are used, although they all allow information to be packaged, sent from a source, and delivered to a destination system.

NetWare, DOS, and OS/2 stations use a network board-specific protocol known as IPX/SPX (**I**nternetwork **P**acket e**X**change/**S**equenced **P**acket e**X**change). Apple Macintosh workstations use AFP (**A**ppleTalk **F**iling **P**rotocol).

See also **NetWare workstation files (IPX.COM).**

CONFIG.SYS

See **Boot files.**

Configuration (hardware)

The equipment used on a network (file servers, workstations, printers, cables, network boards, and routers) and the way the equipment is connected—the physical layout of the network. Hardware configuration includes the following:

- The specific type of hardware installed in or attached to the computer itself, such as disk subsystems, network boards, memory boards, and printer boards.
- A specific set of parameters selected for a board.

See also **Configuration option.**

Configuration option

A combination of settings that specify which resources a network board, coprocessor, or other hardware will use in a computer (file server, router, or workstation). Configuration options can include four settings: interrupt, DMA, base memory, and base I/O address.

The configuration option number indicates the way jumpers or switches should be set on a board. Most network boards are factory set to a default (usually option 0). When more than one network board is installed in a file server or router, configuration options must be chosen carefully so that the boards will use different station resources (interrupts, DMA channels, etc.). If your station doesn't function properly, you may have a resource conflict. Make sure board settings do not conflict with each other or with other hardware.

Interrupt. An interrupt is a signal or call to a specific routine. An interrupt setting allows the hardware in a file server, router, or workstation to send an interrupt signal to the processor. The interrupt signal temporarily suspends the other station tasks while the processor performs the task requested by the interrupting device; after the routine is completed, the processor then continues with the original tasks. Each piece of hardware (serial and parallel ports and network boards) installed in the same computer needs a unique interrupt.

Interrupts are divided into two general types, hardware and software.

A **hardware interrupt** is caused by a signal from a hardware device, such as a printer.

A **software interrupt** is created by instructions from within a software program.

DMA (Direct Memory Access). DMA allows some network boards and the station's memory to transfer data directly from a device to random access memory (RAM) without routing data through the station's microprocessor. The controller signals the processor when the data transfer is complete.

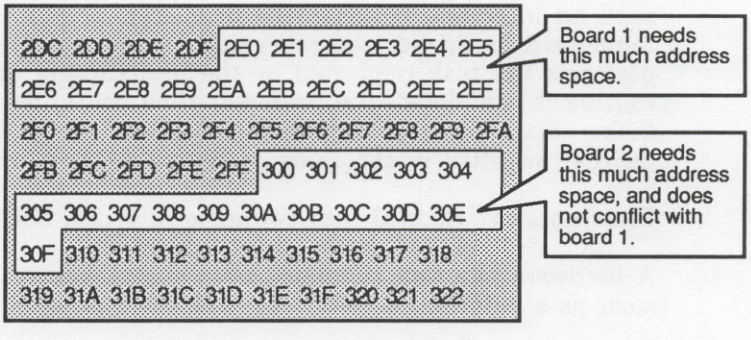
Not all network boards use DMA channels. Check the board's documentation. The DMA controller can handle up to eight devices, each attached to a separate channel. A common source of hardware conflicts is two devices trying to use the same DMA channel.

Base memory and base I/O addresses. Although the base memory address and the base I/O address have separate physical locations in the computer, their function is essentially the same. Network boards are assigned a block of I/O or memory address space in the station so that the board and the operating system can transfer information.

The **base memory address** is used as a buffer to store data. D000, for example, is a common base memory address setting for Arcnet boards. Ethernet boards do not use base memory addresses.

The **base I/O address** is the beginning address of an I/O port. For example, 2E0 is a common base I/O address setting for Arcnet boards, and 300 is a common setting for Ethernet boards.

Preventing configuration conflicts. Make sure that interrupts and DMA channels for separate hardware use unique configuration option numbers. To resolve memory address conflicts, examine the hexadecimal number for base address location in each configuration option. (The file server operating system lists an extra 0 for the number. A complete address such as D0000 on the file server is the same as the segment address D000 for a configuration option.) Make sure the hexadecimal address in the next configuration option is far enough from the first that the address space for one setting does not overlap the space reserved for the next. See the following figure.



I/O address space

INSTALL, WSGEN, and ROUTEGEN keep track of hardware settings as configuration option numbers. Each program warns you of conflicts and prevents you from exiting if you have chosen conflicting hardware options. The configuration option set on the board must match the configuration option chosen during installation.

See also **Node number.**

Connection number

A number assigned to any station that attaches to a file server; it may be a different number each time a station attaches. The file server's operating system uses connection numbers to control each station's communication with other stations. You can find out your connection number using WHOAMI or USERLIST.

Connectivity

The ability to link different pieces of hardware and software (Macintoshes, PCs, minicomputers, and mainframes) in a network environment where resources (applications, printers, etc.) are shared.

See also **Internetwork.**

Console

The console is the monitor and keyboard at which you actually view and control file server or router activity. At the console, you can enter commands to control disk drives, send messages, set the file server or router clock, shut down the file server, and view file server information. Commands you can enter only from the console (for example, MONITOR) are called console commands.

Any unauthorized intrusion into the network from the console can have disastrous effects. An intruder could also take the file server apart and either disable the power-on password protection or remove the hard disks to access the data at leisure. Keep your file server in a physically secure location.

See also **Security.**

Console operator

See **File server console operator.**

Controller

Enables a computer to communicate with another device (such as a hard disk, network board, or tape drive). The controller manages input/output and regulates the operation of its associated device.

See also **SCSI.**

Controller address

The number that the operating system uses to locate the controller on a disk channel. The number is physically set (usually with jumpers) on a hard disk controller. Valid controller numbers are 0 through 7 and can be used in any order. No two controllers on the same channel can use the same address.

See also **Configuration option.**

Coprocessor

See **HBA.**

Core printing

Printing services linked into the operating system (the network core). If core printing is not selected during installation, console commands related to printing will not function.

NetWare v2.2 offers two printing options: core printing and the NetWare Print Server. Core printing allows up to 5 printers to be attached to the file server. The NetWare Print Server allows up to 16 printers to be attached to a dedicated print server, a workstation, or the file server.

See also **Printing;** "Using core printing" in *Using the Network*; the *NetWare Print Server* manual.

Create right

See **Security (Rights security).**

Cylinder

Distinct, concentric storage areas on a hard disk (roughly corresponding to tracks on a floppy diskette). Generally, the more cylinders a hard disk has, the greater its storage capacity.

DDD

Data protection

Consists primarily of maintaining duplicates of the directory table and the FAT (File Allocation Table) and redirecting data from bad blocks to reliable blocks on the hard disk.

Since every network user depends on continual access to data on the file server's hard disks, the most serious file server failures are in the hard disks and their related hardware. Although a hard disk is a reliable and durable storage medium, areas of the hard disk's magnetic surface can, over time, lose the ability to store data reliably. Some of NetWare's built-in protection features are discussed below.

Protecting against directory table and FAT corruption. A hard disk's directory table and FAT are extremely important because they contain the address information the operating system needs to determine where to store or retrieve data. If any of the data storage blocks containing these tables are damaged, some or all of the data on the disk may be irretrievable.

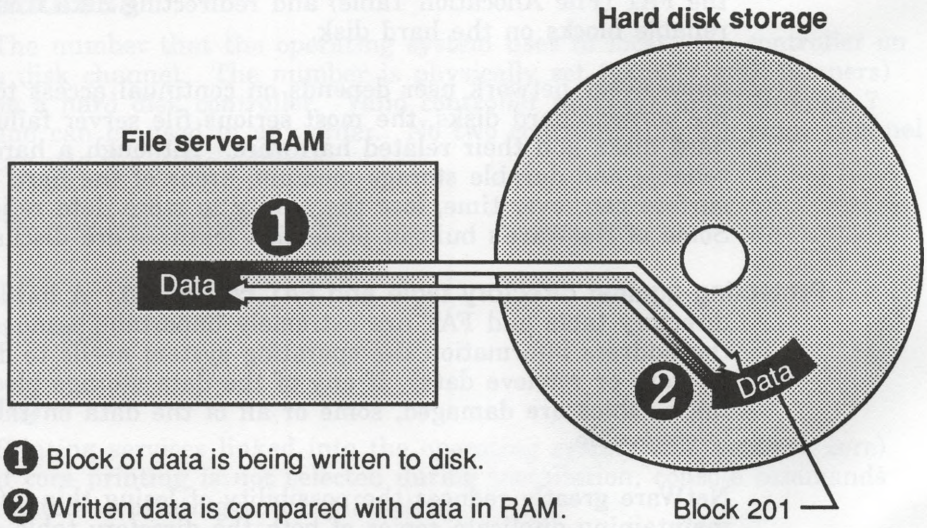
NetWare greatly reduces the possibility of losing this information by maintaining duplicate copies of both the directory table and the FAT on separate areas of the hard disk. If one of the data storage blocks in the original tables is damaged, the operating system automatically switches to the duplicate tables to get the data it needs. The faulty sector is then listed in the disk's "bad block table," and the data it contained is stored in a safe location elsewhere on the disk. Every time the file server is powered on, the operating system performs a consistency check on both sets of directory tables and FATs to verify that the two copies are identical.

Directory table and FAT duplication is an automatic feature of the NetWare operating system. No special steps are required during installation or operation to implement this feature.

Protecting against hard disk surface defects. NetWare hard disks store data in 4KB blocks, specific data storage locations on the disk's magnetic surface. Due to the constant reading and writing of data to the disk, some of these storage blocks can eventually lose their capacity to store data reliably.

NetWare prevents data from being written to unreliable blocks by employing two complementary features, read-after-write verification and Hot Fix. These features, illustrated in the next two figures, enable a hard disk to maintain its data integrity.

Read-after-write verification. When a block of data is written to a hard disk, the data is immediately read back from the disk and compared to the original data still in memory (see figure below).

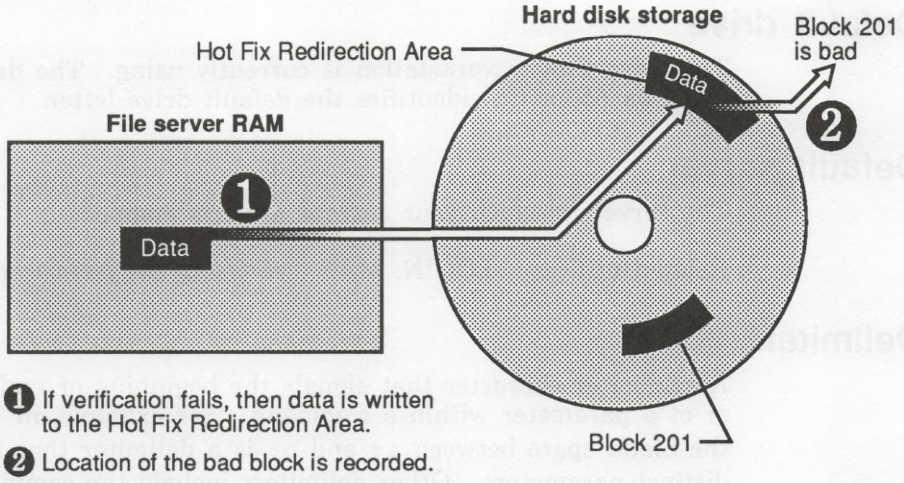


If the data from the disk matches the data in memory, the write operation is considered successful, the data in memory is released, and the next disk I/O operation takes place.

If the data from the disk does not match the data in memory, the NetWare operating system determines (after making appropriate retries) that the disk storage block is defective. The Hot Fix feature redirects the original block of data (still in memory) to the Hot Fix Redirection Area, where the data can be stored correctly.

Hot Fix. A small portion of the disk's storage space is set aside as the "Hot Fix Redirection Area." This area is set up to hold data blocks that are "redirected" there from faulty blocks in the main data storage area of the disk. The Hot Fix feature is always activated on a hard disk, unless the disk fails and is inoperative or the redirection area is full of data blocks redirected from faulty blocks.

Once the NetWare operating system records the address of the defective block in a section of the Hot Fix area reserved for that purpose, the file server will not attempt to store data in the defective block again.



After initial installation, read-after-write verification and Hot Fix are completely user-transparent so that users are not aware of the automatic corrective procedures taking place. The network supervisor or a console operator can view Hot Fix activity in FCONSOLE.

Disk mirroring or duplexing. You can also protect your data with disk mirroring or duplexing. Mirroring stores the same data on two disks on the same controller channel; duplexing stores the same data on two disks on separate controller channels. Duplexing is the preferred method since two channels rarely fail simultaneously.

See also **Cache memory; Directory table; Disk driver; Disk duplexing; Disk mirroring**; "File server installation" and "Maintenance tasks" in *Installing and Maintaining the Network*.

DCB (Disk Coprocessor Board)

See **HBA.**

Dedicated file server

See **File server.**

Dedicated mode

When a file server or router is set up to function only as a file server or router, it runs in dedicated mode.

See also **File server; Nondedicated mode; Router.**

Default drive

The drive that a workstation is currently using. The drive prompt (such as A> or C>) identifies the default drive letter.

Default server

The server to which your current drive is mapped.

Related utilities: LOGIN; MAP (see *Using the Network).*

Delimiter

A symbol or character that signals the beginning or end of a command or of a parameter within a command. For example, in `chkvol a: b:`, the blank space between `a:` and `b:` is a delimiter that marks two distinct parameters. Other delimiters include the comma (,), the period (.), the slash (/), the backslash (\), the hyphen (-), and the colon (:).

Device driver

See **Disk driver; NetWare workstation files.**

Device sharing

Refers to the shared use of centrally located devices (such as printers, modems, and disk storage space) by a number of users. By attaching a device to a file server, which in turn serves several workstations, you can use resources more efficiently.

Direct memory access

See **Configuration option.**

Directory

See **Directory structure.**

Directory attributes

See **Security (Attribute security).**

Directory caching

See **Cache memory.**

Directory entry

Contains basic information for file server files and directories such as

- Name
- Owner
- Date and time of the last update (for files)
- Location of the first block of data on the network hard disk

Directory entries are located in a directory table on a network hard disk. The file server uses directory entries to track file location, changes made to the file, and other related file properties.

The number of directory entries specified during installation determines how many files and directories can be created in a specific volume. Installation offers a default number of maximum directory entries based on the size of the volume. This recommended number is determined by allocating four blocks plus an additional block for every two megabytes of volume size and multiplying the result by 128 entries per block (a 20MB volume would have a default of 1,792 directory entries—14 blocks [4 plus 10] times 128).

Avoid specifying many more than the recommended number of directory entries, especially if the file server will use directory caching and has little excess RAM. If you specify a number that is not a multiple of 128, it is automatically rounded to the next multiple of 128. The maximum number of directory entries can be changed after installation, but you should back up the file server first to avoid losing track of any files, particularly before you decrease the maximum number of directory entries.

See also **Directory table.**

Directory entry table

See **Directory table.**

Directory path

The full directory path on a network lists the name of the file server, the volume, and each directory leading down to the directory you need to access.

See also **Directory structure; Drive mappings.**

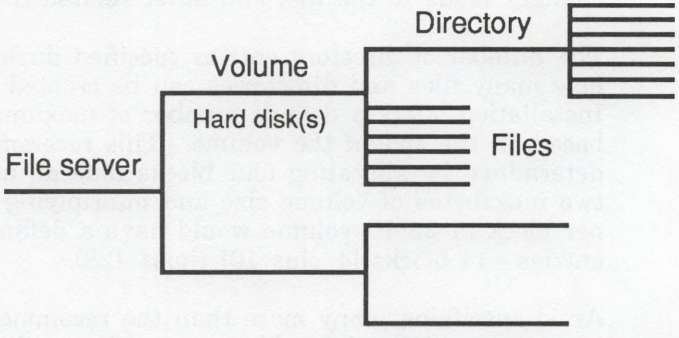
Directory rights

See **Security (Rights security).**

Directory structure

Directory structure is the system used to organize all network files on a file server's hard disk. Each file is given a filename and stored at a specific location in a hierarchical filing system so that files can be located quickly. The levels of this filing system begin with file server, which has one or more

- Volumes, which contain
- Directories, which contain
- Directories (subdirectories) and files



Volumes mark the start of the directory structure. A volume is a logical unit that can be compared to the hard disk of a standalone system. Hard disks may contain more than one volume. You can store directories at the volume level; storing files at this level is possible, but, for security reasons, not recommended.

Directories are places within a volume where you can store files or subdirectories. The term subdirectory is relative: a directory is a subdirectory only in relation to the directory above it. To a directory below it, the same directory is a parent directory.

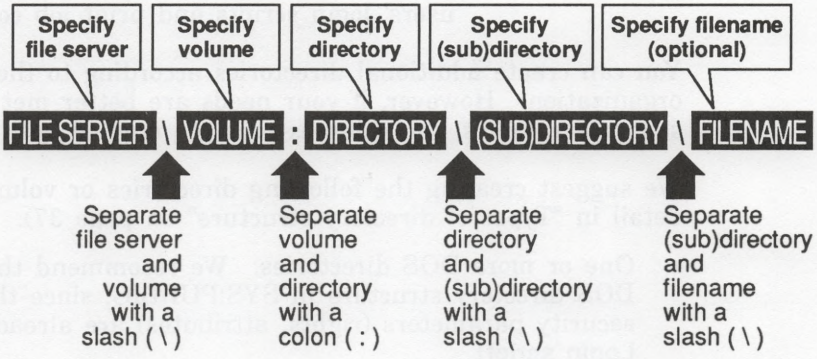
Hierarchically organized directories are like an office filing system, with the levels corresponding to the filing cabinet, file drawer, hanging folders, and manila folders that contain the files.

Files can be created in or copied to any level of the directory structure, from the directory level down. This means that a directory can contain any number of both files and subdirectories.

Each directory is named when it is created. Because each level has a name, the location of any file can be pinpointed by listing the directory name at each level of the directory structure.

Directory levels represent both the directory path and the full name of the directory. Both begin, optionally, with the file server name and then specify volume, directory, and subdirectories (if necessary).

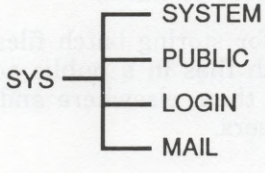
Use the following conventions when naming a directory or specifying a directory path.


Specify file server
Specify volume
Specify directory
Specify (sub)directory
Specify filename (optional)
FILE SERVER \ VOLUME : DIRECTORY \ (SUB)DIRECTORY \ FILENAME
Separate file server and volume with a slash (\ )
Separate volume and directory with a colon (:)
Separate directory and (sub)directory with a slash (\ )
Separate (sub)directory and filename with a slash (\ )

Replace *file server*, *volume*, and *directory* (or *subdirectory*) names with actual names in your specific directory structure. Each can have from 1 to 8 characters. The volume and the root directory (the directory next to the volume) must be separated by a colon (:). Specifying the filename is optional.

As you plan directory structure for networks using more than one workstation operating environment, keep in mind the restrictions and parameters of the different systems if you intend to share files. For example, NetWare allows 255 characters (counting the drive letter and delimiters) in a directory path, but DOS permits only 127 characters. Some applications also restrict the path to the number of characters that will fit the screen width. You should consult the documentation accompanying third-party applications to determine the maximum path length.

Basic directory structure. One volume, SYS, is created automatically during installation; a directory table for SYS is also created. The table contains four predefined directories:



SYS:SYSTEM	Used for system administration; contains operating system files and NetWare utilities reserved for SUPERVISOR.
SYS:PUBLIC	Used for general access; contains NetWare utilities for regular network users.
SYS:LOGIN	Contains utilities necessary for logging in.
SYS:MAIL	Used by NetWare-compatible mail programs. This directory also contains an ID number subdirectory for users' login scripts and print job configurations.

You can create additional directories according to the needs of your organization. However, if your needs are better met by creating separate volumes, the volumes must be created with INSTALL.

We suggest creating the following directories or volumes (discussed in detail in "Types of directory structure" on page 37):

- One or more DOS directories. We recommend that you create your DOS directory structure in SYS:PUBLIC, since the appropriate security parameters (rights, attributes) are already set up (see **Login script**).
- One or more application directories. Create a separate directory for each application.
- A "home" or username directory for each user. If you want users to have personal workspace, you can create a separate directory (or volume) for this purpose.

You may also find the following kinds of directories useful:

- Work or project directories. If you want users to have group workspace or if you want to store completed application data files, you can create a directory for each project. You may want to create them in separate volumes to simplify backup.
- A common directory in the SYS volume (or a HOME or a WORK volume) to serve as an intermediate point in transferring files. (The group EVERYONE should be assigned the rights necessary to copy files to and from this directory. If you do not want GUEST to have access to this directory, delete GUEST from the group EVERYONE and assign GUEST only the rights you want temporary users to have.)
- A directory for storing batch files and utilities. If you do not want to store batch files in a public access directory, you can create a directory for them elsewhere and assign rights to groups or to individual users.

How directories are accessed. Although you can use DOS commands to access directories, NetWare provides a more direct way. Like DOS, NetWare uses the letters of the alphabet to represent various data storage locations, or drives. In DOS, drive A refers to the first floppy diskette drive and drive B to the second floppy diskette drive (if there is one). Depending on your workstation type, drive C could be a local hard disk.

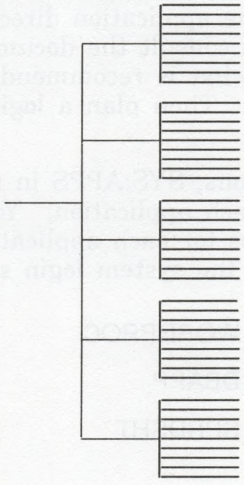
Unlike a workstation's physical drives, network drives are logical. They can be configured to "point" to a particular location in the directory structure or mapped to a particular directory.

Each workstation can use the 26 letters of the alphabet as *pointers*. You can map or point all these drives to a particular directory path (name) in the directory structure. The NetWare default is for the first letters of the alphabet (A through E) to point to local workstation drives. These local drives point to the root directory created on each floppy diskette.

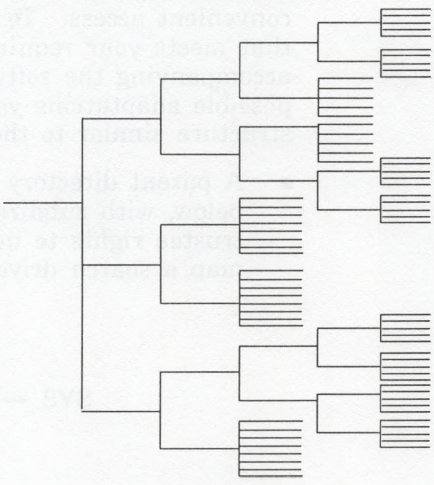
NetWare recognizes three types of drives: network, search, and local. Network and search drive mappings can be set with MAP or SESSION.

Types of directory structure. All directory structures are tree structures, but trees may have different proportions. A directory structure may be relatively shallow with many directories created at the volume (root) level or deep if you limit the number of directories at the root and create several levels of directory structure. The general principle is to keep the directory structure clean and logical. Keeping the structure relatively shallow (no more than five levels deep) generally increases its usability.

Shallow directory structure



Deep directory structure



Consider the following guidelines as you plan directory structure:

- Group your files logically. Plan subdirectory levels for natural subcategories.
- Limit the number of files in each directory.
- Determine which method allows the fewest characters in a directory path. You may need to plan either shorter directory names or a shallower directory structure.

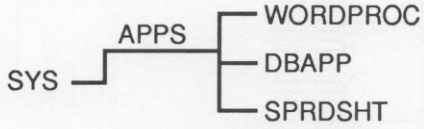
Types of directories. You can create directories for either executable files or data files. As network administrator, you must determine which types of directories best fit the needs of your network.

DOS directories. If your network uses DOS workstations, DOS is installed on the network by copying DOS files into network directories. You must create one or more DOS directories, copy DOS files into the directories, and then include a search drive mapping (usually Search2) to the directories in the system login script. You may want to provide a similar setup for OS/2 workstations. Macintosh workstations do not need such a setup. (For more information, see **Login script**.)

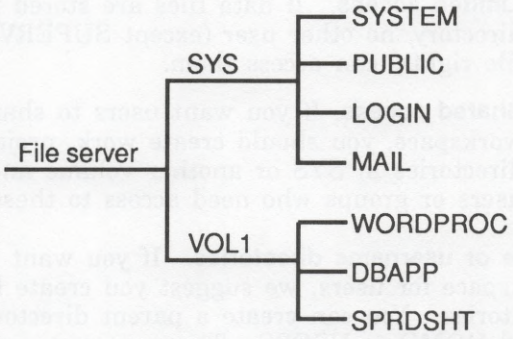
If your network includes different types (brands) of workstations, you may need to create separate directories for different types of DOS. For example, if you are using DOS v3.30 but have both COMPAQ and IBM workstations, you will need to create a directory for each combination (DOS/COMPAQ/V3.30 and DOS/IBM/V3.30) instead of simply creating a directory for 3.0. In this situation, also include the LONG MACHINE TYPE variable in the workstation's SHELL.CFG file so that you can have a mapping to the appropriate DOS directory.

Application directories. Although applications can be accessed from local drives, installing them on the network provides the most convenient access. To determine the application directory structure that meets your requirements, first consult the documentation accompanying the software to see what is recommended or what possible adaptations you can make. Then plan a logical directory structure similar to the following:

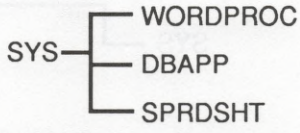
- A parent directory for applications, SYS:APPS in the example below, with subdirectories for each application. You must assign trustee rights to users or groups for each application directory and map a search drive for each in the system login script.



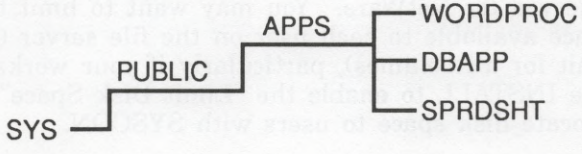
- A separate volume (VOL1 in the example below) for applications, subdivided at the root into separate directories for each application. You must assign users or groups trustee rights for each application directory and map search drives in the system login script. This solution hides applications from GUEST and simplifies backup.



- A separate directory off the SYS volume for each application. You must assign users trustee rights for each directory and map a search drive for each in the system login script. (Some applications write files to the root. If, for security reasons, you don't want users to work at the root, use MAP ROOT to map a drive to a fake root, in this case, a directory off SYS in which the user can be assigned rights. See **Fake root.**)



- A parent directory for applications, APPS, in SYS:PUBLIC. Because the group EVERYONE has Read and File Scan rights in SYS:PUBLIC, you do not need to assign trustee rights or map a search drive. However, EVERYONE and GUEST can see and use all applications. Use this directory structure only if you want all users (particularly GUEST) to have access to all applications.

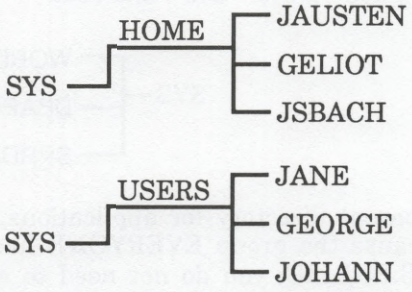


We do not recommend installing applications in SYS:PUBLIC unless you create a subdirectory for each application. Upgrading a network is more complicated if you mix NetWare utilities with application files because filenames may conflict causing one file to overwrite the other (two files with the same name can't coexist in a directory).

Application data files can be created and stored in personal workspace in the home or username directory or in group workspace in separate work, project, or database record directories (these directories are also explained below). You will need to decide whether limited or shared access is better in your particular situation.

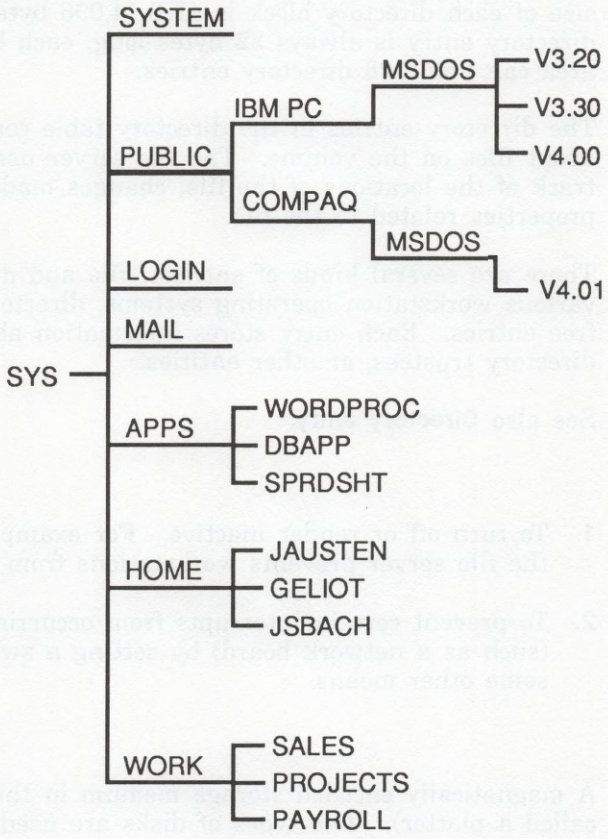
- **Limited access.** If data files are stored in each user's username directory, no other user (except SUPERVISOR or managers assigned file rights) can access them.
- **Shared access.** If you want users to share data in a group workspace, you should create work, project, or database record directories in SYS or another volume and assign trustee rights to users or groups who need access to these directories.

Home or username directories. If you want to provide personal workspace for users, we suggest you create home or username directories. You can create a parent directory in the SYS volume called HOME or USERS. Then you can create a subdirectory for each user. The name of each subdirectory should be the username. NetWare allows usernames of up to 47 characters, but DOS will display only 8 characters in a one-level directory name. The username is usually composed of either the initials and surname or the given name. See the following examples for both kinds of username directories.



Limiting volume and directory size. A volume is defined during installation; the default is the entire hard disk. A NetWare volume is, therefore, a physical amount of hard disk storage space measured in megabytes and reserved for NetWare. You may want to limit the amount of disk space available to each user on the file server (you can set a blanket limit for all volumes), particularly if your workstations have hard disks. Use INSTALL to enable the "Limit Disk Space" parameter and then allocate disk space to users with SYSCON.

Charting directory structure. To plan or to keep track of your directories, make a chart similar to the following. You do not need to create any directories in SYS:SYSTEM, SYS:LOGIN, or SYS:MAIL (when you create each user, a subdirectory is automatically created to store the user login script and print job configurations in SYS:MAIL).



See also **Directory table; Drive mappings; Security (Rights security).**

Related utilities:

DOS
: CD (Change Directory); DIR; MD (Make Directory); RD (Remove Directory).

NetWare
: CHKVOL; FILER; FLAGDIR; LISTDIR /S; MAP; NDIR *path*; RENDIR; SYSCON (see *Using the Network*).

Directory table

Table located on each of the network volumes that contains the directory entries for that volume.

The directory table (a file) occupies one or more directory blocks. The size of each directory block is 4KB (4,096 bytes of data). Since a directory entry is always 32 bytes long, each block in the directory area can hold 128 directory entries.

The directory entries in the directory table contain basic information about files on the volume. The file server uses the entries to keep track of the locations of the file, changes made to the file, and other properties related to the file.

There are several kinds of entries: file and directory entries for various workstation operating systems, directory trustee entries, and free entries. Each entry stores information about files, directories, directory trustees, or other entities.

See also **Directory entry.**

Disable

1. To turn off or render inactive. For example, DISABLE LOGIN at the file server prevents workstations from logging in.

2. To prevent certain interrupts from occurring in a processing unit (such as a network board) by setting a switch or a jumper, or using some other means.

Disk

A magnetically encoded storage medium in the form of a plate (also called a platter). Two types of disks are used with personal computers:

- **Hard disks** have a metallic base and are usually installed in a computer or a disk subsystem. In some cases, this storage medium is removable.
- **Floppy disks** (diskettes) have a polyester base and are always removable.

Related utilities: DISMOUNT; MOUNT (see *Using the Network*).

See also **Data protection; Hard disk; Partitions.**

Disk controller

A hardware device that controls how data is written to and retrieved from the disk drive. The disk controller sends signals to the disk drive's logic board to regulate the movement of the head as it reads data from or writes data to the disk.

See also **SCSI.**

Disk coprocessor board

See **HBA.**

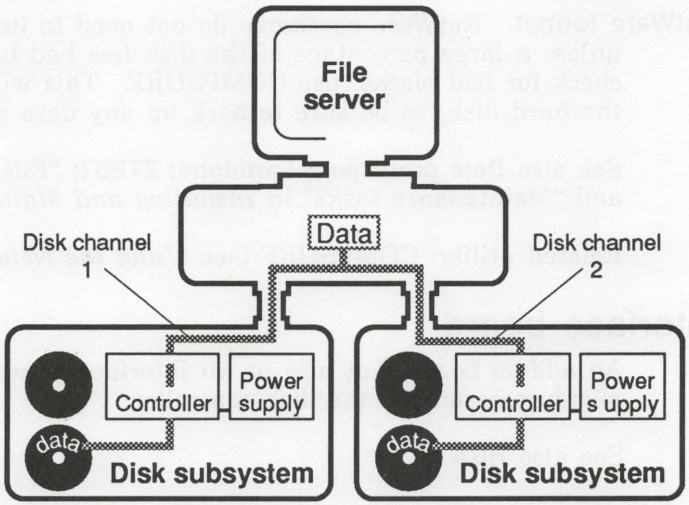
Disk driver

Software routine that forms the interface between the NetWare operating system and the hard disk(s). The disk driver talks to a hard disk controller that is connected to the disk drive(s). The driver is linked into the NetWare operating system during installation.

Disk duplexing

Copying data onto two hard disks, each on a separate disk channel. Disk duplexing protects data against the failure of a hard disk or of the hard disk channel between the disk and the file server. (The hard disk channel includes the disk controller and interface cable.)

If any component on one channel fails, the other channel continues to operate normally. The operating system sends a warning message to indicate the failure. Restore duplexing protection as soon as possible.



Disk duplexing

Note: Duplexing alone does not ensure data protection. If both hard disks fail at the same time, you will still lose your data. Therefore, you need to back up your data on a regular basis. Use NBACKUP or a third-party backup utility.

Disk duplexing allows the same data to be written to all disks simultaneously. Since the disks are on different channels, data transfer is faster than with disk mirroring, where data is written to the disks sequentially over the same channel.

Disk duplexing also allows "split seeks." This feature sends read requests to whichever disk in the pair can respond first. Multiple read requests are also split between the duplexed disks for simultaneous processing.

See also **Disk mirroring**; "File server installation" and "Maintenance tasks" in *Installing and Maintaining the Network.*

Disk formatting

Dividing a disk into sectors so that it can receive data from the computer's operating system. Many hard disks come formatted. A NetWare file server works with two kinds of hard disk formatting: DOS and NetWare.

DOS format. This format allows a file server to boot from a DOS partition. (This is optional since a file server can also be booted from a diskette to run NetWare.) You can set up a DOS partition with INSTALL. You must then use DOS FDISK and FORMAT (see your DOS manual).

NetWare format. NetWare partitions do not need to be formatted initially, unless a large percentage of the disk has bad blocks. If you need to check for bad blocks, use COMPSURF. This will destroy any data on the hard disk, so be sure to back up any data you want to save.

See also **Data protection; Partitions; ZTEST**; "File server installation" and "Maintenance tasks" in *Installing and Maintaining the Network.*

Related utility: COMPSURF (see *Using the Network*).

Disk interface board

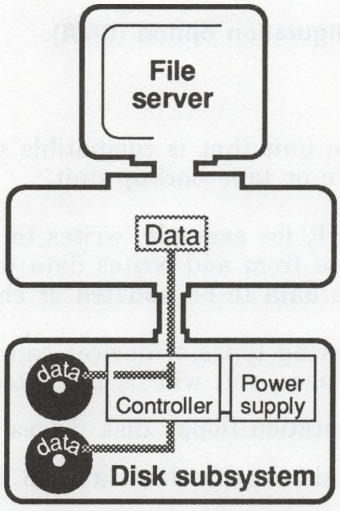
An add-on board that acts as an interface between the host microprocessor and the disk controller.

See also **HBA.**

Disk mirroring

The duplication of data from the NetWare partition on one hard disk to the NetWare partition on another hard disk.

When you mirror disks, two hard disks on the same channel are paired (see the illustration below). Blocks of data written to the original (primary) disk are also written to the duplicate (secondary) disk. The disks operate in tandem, constantly storing and updating the same files.



Disk mirroring

Note: Mirroring alone does not ensure data protection. If both hard disks fail at the same time, you will still lose data. Use NBACKUP or a third-party backup utility to back up your data on a regular basis.

If one of the disks fails, the other continues to operate without data loss or interruption. The operating system sends a warning message to indicate the failure so that mirroring protection can be restored as soon as possible.

Because disk mirroring duplicates disks on the same channel, it does not protect against failures that may occur along the channel between the disks and the file server. A problem in the channel would cause a failure in both disks.

See also **Disk duplexing;** "File server definition" and "Maintenance tasks" in *Installing and Maintaining the Network.*

Disk partitions

See **Partitions.**

Disk subsystem

An external unit that attaches to the file server and may contain hard disk drives, a tape drive, or both. The disk subsystem gives the file server more storage capacity.

DMA

See **Configuration option (DMA).**

DOS device

A storage unit that is compatible with the IBM disk format—usually a disk drive or tape backup unit.

NBACKUP, for example, writes to a DOS device. Because the utility reads data from and writes data to the media, the DOS device must allow the data to be updated or changed.

The following types of devices can be used. If the device runs out of storage space, you will be prompted to insert another tape or disk.

- Workstation floppy disk drives
- Tape drives that have a DOS device driver
- Optical drives that have read-and-write capability and a DOS device driver

The following can also be used as DOS devices; if you use them, however, you must make sure the data selected for the backup session will fit on the device:

- Workstation hard disk drives
- Network drives
- An optical drive for a WORM drive that has a DOS device driver

DOS directories

See **Directory structure; Drive mappings; Login script.**

DOS setup routine

Sets up the system configuration for your workstation or file server. The routine records the system's built-in features (boards, hard drives, disk drives, ports, math-coprocessor) and the available system memory. You can also set date and time, a password, and keyboard speed. The system configuration is accessed from the reference diskette (for IBM PS/2 systems) or from the user diagnostics diskette (for most other systems). Instructions for running the DOS setup routine are usually contained in the introduction to your system's operations guide.

DOS version

Different machine types (such as HP, IBM, or Corona) use different versions of DOS that are generally not compatible. You need to inform the NetWare shell about the DOS version(s) and the workstation type(s) used, since the shell is built around DOS. Based on the information embedded in the shell, the shell descriptors (long machine name, short machine name, and DOS version) are read by the login script.

Since all DOS versions have identically-named utilities and command interpreters, you cannot place the files for different DOS versions in the same directory. You must create a DOS directory for each workstation type/DOS version you will use on your network and copy the DOS files into it. NetWare installation requires DOS v3.0 or above.

See also **Directory structure; Login script; NetWare workstation files.**

Down time

In a NetWare UPS system, the number of seconds the file server will wait while running on the UPS before downing itself. Down time should give users ample time to close or save their files and log out.

See also **Power conditioning; UPS monitoring; Wait time.**

Drive

Drives can be physical or logical.

- **A physical drive** is a storage device (such as a hard disk or tape drive) that data is written to and read from. A drive that is physically attached to a workstation is called a local drive.
- **A logical drive** is a pointer to or an identification of a specific directory located on a hard disk. Network drives read data from a specified directory on the network rather than from a local disk.

Drive mappings

Drive mappings provide direct access to particular locations in the directory structure. They are a "shorthand" method for accessing directories on a disk. Instead of typing in the complete pathname of a directory that you want to access, you can simply enter a drive letter that has been assigned to that directory.

Types of drive mappings

NetWare recognizes two types of drives (physical drives and logical drives) and three types of drive mappings (local, network, and search drive mappings).

Local drive mappings. Local drive mappings point to physical disk drives installed in or attached to individual workstations. These disk drives may be floppy diskette drives or hard disk drives. The directory structure accessed with a local drive letter depends on either the contents of the diskettes inserted into the drive or the contents of the local hard disk.

By default, NetWare reserves a certain number of drive letters (A, B, C, and so on) for local workstation drives. The first network drive is usually F. (If you want to change the number of drive letters reserved for local drives, see your DOS manual for an explanation of the DOS LASTDRIVE command used in the DOS CONFIG.SYS file.)

Network drive mappings. A network drive points to a specific (but logical) location in the directory structure on the file server's hard disk and serves the same function as a bookmark; it allows a user direct access to a particular location. The first network drive is usually F.

To map a network drive to a directory, use the MAP command to assign a drive letter to represent the logical drive; then specify a particular directory path that leads to the desired point in the directory structure.

For example, you could type the following command at the command line or include it in the login script:

```
MAP G:=BACH\SYS:HOME\GEORGE
```

The drive letter G would now represent the directory. You can access BACH\SYS:HOME\GEORGE by typing the drive letter followed by a colon (instead of the complete directory path):

```
G: <Enter>
```

If you want the directory path displayed, set the DOS prompt in your system login script by entering

```
PROMPT "$P$G"
```

The DOS prompt would then be displayed (volume level omitted) as

```
G:\HOME\GEORGE>
```

When you use MAP at the command line, the drive remains mapped until you log out. If you want the same drive mappings each time you log in, include them in a login script. (See **Login script.**)

Search drive mappings. A mapped search drive allows you to execute files that are not in your current directory.

When you specify a file you want to execute, the file server looks for the file in the directory to which you are currently mapped (your location in the directory structure). If the file is not in that directory, you would ordinarily see the message "File not found" or "Bad command or filename." By mapping a search drive to the directory that contains the files, however, you can access these files even though you are working in another directory. When you request a file and the system cannot find it in your current directory, the system looks in any directory to which a search drive is mapped.

For example, suppose you need to access DOS or an application from other directories. When the file is not found in your current (default) directory, the system continues searching, following the numerical order of the search drives, until the file is found or cannot be located. (Use SMODE to specify where the system will look for data files and under what conditions the data files can be used.)

Search drives are numbered (although they also have drive letters). We recommend assigning frequently used application or DOS directories to search drives in numerical order, beginning with Search1. Usually the first search drive (Search1 or S1) is also network drive Z; the second search drive (S2) is network drive Y, and so on in reverse alphabetical order.

NetWare allows each user to assign as many as 16 of the workstation's 26-drive total as search drives.

Assigning drive letters. You have considerable flexibility in assigning drive letters. As supervisor, you select the drive letters for the drive mappings in the system login script. Use them in alphabetical sequence, or use them as an aid to users' memory (for example, H for historical files or P for a payroll directory).

Network users who either work at the command line or who want to modify their individual login scripts can assign any unallocated drive letters. Each network user can assign different directories to a particular drive letter. For example, one user might map drive J to SYS:PROJECTS\PLANS, while another user might map drive M to the same directory.

Since network users can assign drive letters differently, you should specify the full directory path when you tell users where a particular file is located.

Viewing drive mappings. When you log in to the file server for the first time (before system and user login scripts are created), a list of default drive mappings similar to the following appears:

```
Good morning, SUPERVISOR.

Drive A: maps to a local disk.
Drive B: maps to a local disk.
Drive C: maps to a local disk.
Drive D: maps to a local disk.
Drive E: maps to a local disk.
Drive F:= BACH\SYS:    \SYSTEM
         -----
SEARCH1: =Z:.[BACH\SYS:    \PUBLIC]
SEARCH2: =Y:.[BACH\SYS:    \]

F:>
```

As you can see in this example from the file server BACH, drives A through E are mapped to local disks (the NetWare default). The first one or two local drive mappings usually correspond to floppy diskette drives.

Drives F, Y, and Z are network drive mappings. Drive F is the first network drive (NetWare default) and, for SUPERVISOR, it is mapped to BACH\SYS:SYSTEM. Drive Z is a search drive mapped to the SYS:PUBLIC directory. This search drive mapping allows you to access the NetWare utilities in the SYS:PUBLIC directory from any point in the directory structure. (Drive Z is mapped to SYS:PUBLIC. When you install DOS on the network, the DOS directory structure will be added to the path for drive Y.)

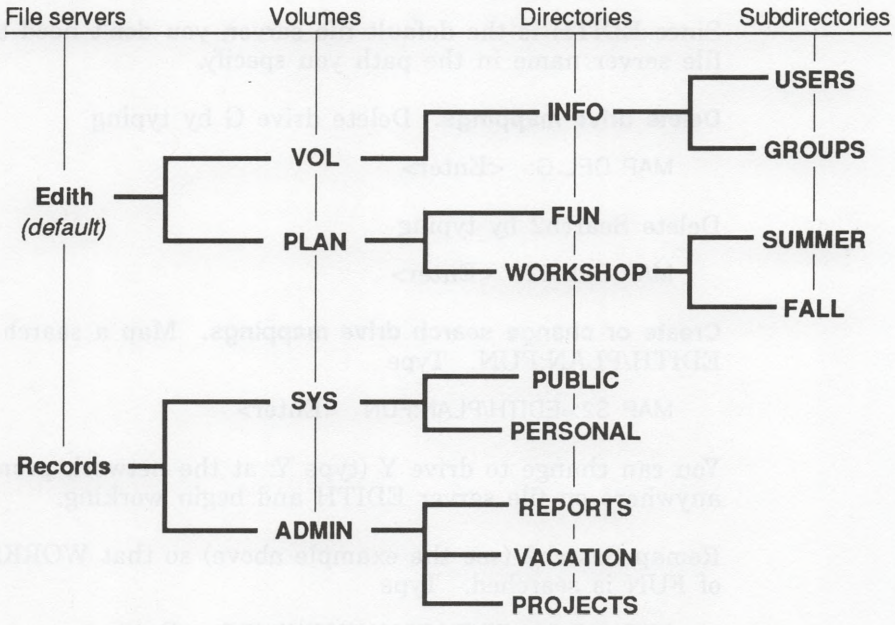
The last line of the screen display, F:> or F:\SYSTEM> indicates your current or "default" directory (the directory to which you are currently mapped). (The prompt is displayed as F:\SYSTEM> only if you first set the prompt to "PG" at the command line, in the AUTOEXEC.BAT file, or in a login script.)

You can display your current drive mappings at any time by entering MAP at the prompt.

Examples. Assume the following:

- Your available network drives are G, H, J, and K.
- Your first search drive (assigned the letter Z) is mapped to RECORDS/SYS:PUBLIC, so your next available search drive is Search2.

Refer to the hypothetical directory structure shown in the following illustration as you read through the examples that follow.



View current drive mappings. Type

MAP <Enter>

View the mapping for drive G. Type

MAP G: <Enter>

Create or change network drive mappings. Make drive G your default drive and map it to your WORKSHOP directory by typing

MAP G:=EDITH/PLAN:WORKSHOP <Enter>

You can access the WORKSHOP directory anytime by changing to drive G at the command line. You can also map drives to other file servers as long as you are attached to them.

Map drive H to server RECORDS, volume ADMIN, directory PROJECT by typing

MAP H:=RECORDS/ADMIN:PROJECT <Enter>

As long as your workstation is attached to server RECORDS, drive H will be mapped to the PROJECT directory.

Remap your default drive to EDITH/VOL:USERS by typing

```
MAP VOL:USERS  <Enter>
```

Since EDITH is the default file server, you don't need to include the file server name in the path you specify.

Delete drive mappings. Delete drive G by typing

```
MAP DEL G:  <Enter>
```

Delete Search2 by typing

```
MAP DEL S2:  <Enter>
```

Create or change search drive mappings. Map a search drive to EDITH/PLAN:FUN. Type

```
MAP S2:=EDITH/PLAN:FUN  <Enter>
```

You can change to drive Y (type Y: at the network prompt) from anywhere on file server EDITH and begin working.

Remap Search2 (see the example above) so that WORKSHOPS instead of FUN is searched. Type

```
MAP INS S2:=EDITH/PLAN:WORKSHOP  <Enter>
```

Map a drive to a fake root directory. Some applications must be run from a "root" directory. For security reasons, users would not usually be assigned rights at the root directory level. To compensate, NetWare allows you to install the files in a subdirectory and designate the subdirectory as a "fake" root. For example, user JON, who has been assigned appropriate directory and trustee rights, needs to run an application (installed in the FALL subdirectory) that requires a root directory. Create the fake root by typing

```
MAP ROOT G:=WORKSHOP/FALL  <Enter>
```

Delete the fake root by remapping the search drive. For example, type

```
MAP ROOT G:  <Enter>
```

Map the next available network drive to a directory. If you do not know which drives you have already mapped but want to map the next available drive to RECORDS/ADMIN:VACATION, type

```
MAP N RECORDS/ADMIN:VACATION  <Enter>
```

Accessing directories from login scripts. You can use MAP to create drive mappings in both system and user login scripts. For example, to give all users access to a work directory you have created, you could enter a command similar to the following in the system login script.

```
MAP G:=SYS:REPORTS
```

Or, if the directory was created for a particular group, you could enter a command similar to the following in the system login script.

```
IF MEMBER OF "MARKETING" THEN MAP G:=SYS:REPORTS
```

For efficiency, a user login script should have drives mapped to directories used only by that particular user.

Use either MAP or MAP INSERT to map a search drive to a directory created for batch files (MAP INSERT does not overwrite any current drive mappings).

```
MAP S5:=SYS:BATCH
MAP INS S5:=SYS:BATCH
```

Login scripts and DOS directories. Use one of the following, depending on the directories you plan, to map a search drive to DOS directories.

```
MAP S2:=SYS:PUBLIC\%MACHINE\%OS_VERSION
MAP INS S2:=SYS:PUBLIC\%MACHINE\%OS_VERSION
```

Whenever you enter a DOS command, the file server will automatically look first in your current directory. If the DOS file is not found, the file server looks in the first search drive. In this case, the system will find the DOS files in the second search drive and the command will be executed.

Login scripts and application directories. Mapping a search drive to application files depends on the directory structure you created for applications. Suppose, for example, that the word processing files are located in SYS:APPS\WORDPROC. The system login script could map the third search drive (S3) to that directory so users can load word processing files stored in other directories.

If you form user groups according to application use, a conditional command in the system login script could map a search drive to the different application directories, similar to the following.

```
IF MEMBER OF "WORDPROC" THEN BEGIN
MAP INS S16:=SYS:APPS\WORDPROC
END
```

As long as you use MAP INSert, you can map Search16 conditionally to two or more application directories simultaneously. This procedure is more efficient if you put a series of mappings in the reverse order of frequent use (list the least frequently used application group first and the most frequently used application group last).

Because MAP INSert inserts a new search drive using the next available number in the ordered sequence of search drives, one mapping will not overwrite another in the following example.

```
IF MEMBER OF "WPUSERS" THEN
MAP INS S16:=SYS:APPS\WORDPROC

IF MEMBER OF "DB" THEN MAP INS S16:=SYS:APPS\DBAPP
```

Network drives and generic mappings. You can use generic mappings for network drives by designating them *1, *2, and so on. If your workstation has two local drives, A and B, then *1 would map to one of two drives:

- The first drive beyond the drive specified by LASTDRIVE in CONFIG.SYS (see the DOS manual)
- Drive F (except DOS 2.*x*), if no LASTDRIVE = *drive* has been specified

Suppose you have a variety of workstations, but want to map the first network drive to individual users' home directories. In this case, you would include a mapping similar to the following.

```
MAP *1:=SYS:USERS\%LOGIN_NAME
```

If you want to map the next drive letter to a work directory, you could include a mapping similar to the following.

```
MAP *2:=SYS:SALES\PROJECTS
```

See also "Logging in and out" in *Using the Network.*

See also **Directory structure; Fake root; Login script.**

Related utilities: MAP (see *Using the Network).*

Driver

See **Disk driver; NetWare workstation files (LAN driver).**

Duplexing

See **Disk duplexing.**

Dynamic memory

The most common form of memory, used for RAM, with an access speed ranging from about 60 to 150 nanoseconds. Dynamic memory requires a continuous electrical current (all data is lost when the power supply is shut off). Frequently saving files to disk helps preserve data. Downing a NetWare file server allows the operating system to write data in memory to disk to prevent any data loss from loss of power.

NetWare v2.2 uses four dynamic memory pools of operating system memory:

- Pool 1, a section of DGROUP memory, is used for miscellaneous, short-term memory tasks such as building replies to user NCP (NetWare Core Protocol) calls.
- Pool 2 holds file handles and locking.
- Pool 3 holds router information tables.
- Pool 4 holds drive mappings (directory handles).

Dynamic memory pools

See **Dynamic memory.**

EEE

Effective rights

See **Security (Effective rights).**

Elevator seeking

Organizes the way data is read from hard disks and logically organizes disk operations as they arrive at the server for processing.

A queue is maintained for each disk driver operating within the server. As disk read and write requests are queued for a specific drive, the operating system sorts incoming requests into a priority based on the drive's current head position. As the disk driver services the queue, subsequent requests are located either in the vicinity of the last request or in the opposite direction. Thus, the drive heads operate in a sweeping fashion, from the outside to the inside of the disk.

Elevator seeking improves disk channel performance by significantly reducing disk head thrashing (rapid back-and-forth movements of the disk head) and by minimizing head seek times. Imagine how inefficient an elevator would be if the people using it had to get off the elevator in the same order as they got on.

Embedded SCSI

A hard disk that has a SCSI (Small Computer System Interface) and a hard disk controller built into the hard disk unit.

See also **SCSI.**

Enable

1. To turn on, especially to restore a feature that has been disabled.

2. To place in a state that will allow certain interrupts to occur in a processing unit (such as a network board). Interrupts are usually enabled by setting a switch or a jumper.

Encrypted passwords

Passwords that have been scrambled before being stored on the file server to prevent an intruder from viewing or copying them. NetWare encrypts the password at the workstation before it is transmitted to the file server. This prevents intruders from monitoring the password as it passes over the transmission lines.

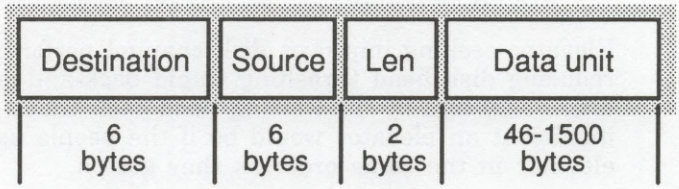
See also **Bindery; Password.**

Erase right

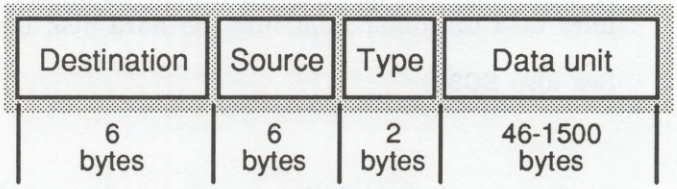
See **Security (Rights security).**

Ethernet configuration

In an Ethernet environment, stations communicate with each other by sending data in packets along an Ethernet cabling system. The IEEE 802.3 standard and the Ethernet II (or Ethernet) standard use different frame formats, as shown below.



IEEE 802.3 frame



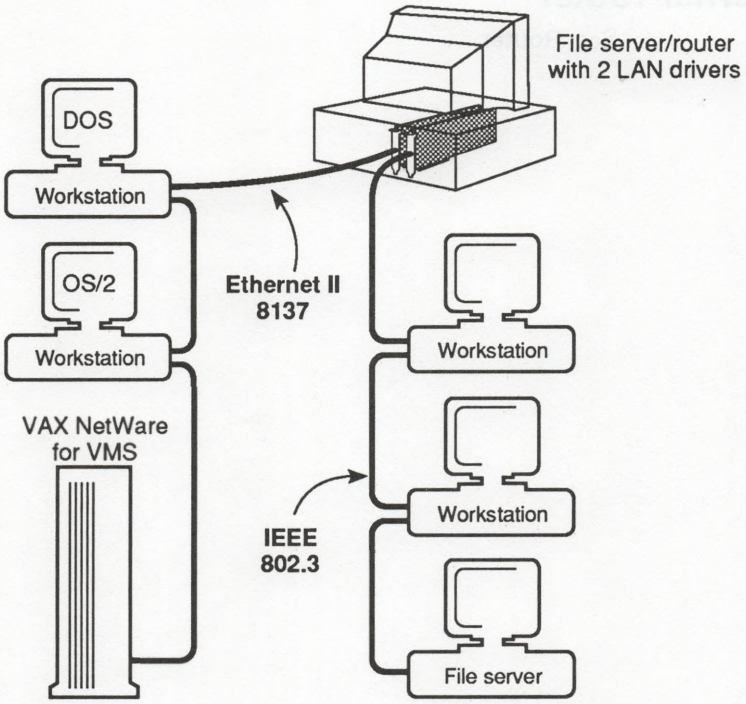
Ethernet II frame

Ethernet II frames contain a unique protocol ID or PID (represented in the "Type" field of the frame) that IEEE 802.3 frames do not contain. Stations using the different standards can co-exist on the same Ethernet cabling system. Ethernet II stations using different protocol numbers on an Ethernet II cabling system can also co-exist, but they cannot communicate with each other.

NetWare uses the IEEE 802.3 standard by default. However, you can configure file servers, workstations, and routers to use the Ethernet II standard. To do this, you must use ECONFIG or, if you are using ODI shells, place the following line in NET.CFG under the appropriate Link Driver statement:

```
frame ethernet_II
```

The following diagram illustrates how multiple networks can be configured on an Ethernet cabling system.



EVERYONE

See **Groups; User.**

Execute Only attribute

See **Security (Attribute security).**

Expanded memory shell

See **NetWare expanded memory shell.**

Extended memory requirements

See **File server.**

Extended memory shell

See **NetWare extended memory shell.**

External router

See **Router.**

FFF

Fake root

A subdirectory that functions as a root directory, where you can safely assign rights to users.

Note: Fake roots only work with NetWare shells included with NetWare v2.2 and above. If you use older versions of the workstation shell, you will not be able to create fake roots.

Some applications cannot be run from subdirectories; they read files from and write files to the root directory. However, for security reasons, users usually should not be assigned rights at the root directory level. If you must use an application at the root, you can install the files in a subdirectory and designate the subdirectory as a fake root directory, using MAP (at the prompt or in the system or user login script); for example, type

```
MAP ROOT S16:=SYS:APPS\NONETAPP
```

You cannot use DOS CD (change directory) at the fake root to return to the original root. To change the fake root back to the original root, remap the drive.

See also **Login script; Security.**

FAT (File Allocation Table)

An index to one or more disk allocation blocks in which a file is located. Each volume contains a FAT which is accessed from the directory table. The entire FAT is cached in server memory, allowing the server to quickly access any disk allocation blocks of data in the volume. Because one file may be in any number of disk allocation blocks spread over the disk, the FAT links the file together.

NetWare divides each volume into blocks of 4KB (4,096 bytes) for file storage. A file larger than 4,096 bytes spans multiple blocks that may not be adjacent.

Entries in the FAT correspond to the blocks for that volume. The first entry in the FAT corresponds to the first block on that volume, the second entry corresponds to the second block, etc.

For example, if one file consists of six blocks (blocks 0, 2, 4, 6, 7, and 9), block 0 indicates that the file begins in this block. It also contains a link to the next block for the file, block 2. Block 2 contains the link to the next block, block 4. The last block, block 9, contains the end of file marker. When you want to retrieve a file, NetWare searches through the FAT entries until it finds all the FAT entries and corresponding blocks for the file you requested.

Turbo FAT. An index NetWare v2.2 creates to group all the FAT entries corresponding to a file larger than 262,144KB (64 blocks, each 4,096KB) and the corresponding number of FAT entries. The first entry in the turbo FAT index table consists of the first FAT number of the file. The second entry consists of the second FAT number of the file, etc. The turbo FAT enables a large file to be accessed quickly.

Theoretically, if RAM were used only to cache directories, a server could cache up to 2,000,000 FAT entries. This value is determined by dividing 16MB of total memory by 8 bytes per FAT entry. Since each FAT entry indexes one 4KB (4,096 bytes) disk allocation block, the server could access 8 billion bytes of disk storage. NetWare supports up to 32 volumes, each one with a maximum size of 255MB.

See also **Cache memory; Data protection.**

Fault tolerance

See **SFT.**

Ferro-resonant isolation transformer

See **Power conditioning.**

File Allocation Table

See **FAT.**

File attributes

See **Security (Attribute security).**

File caching

See **Cache memory.**

File extensions

DOS files can have an 8-character filename followed by a period and a 3-character file extension. While most extensions are arbitrarily assigned by users or companies, some extensions are reserved for special purposes or circumstances:

- The extensions .COM, .EXE, or .BAT enable a file to execute a command, program, or batch file, respectively.
- The extensions .ERR and .DAT indicate that the file contains an error log file or an ASCII text file, respectively.
- Some extensions identify the file format (such as .ASC, .BIN, .GIF, .DFX, or .RFT).
- Some extensions are assigned by the manufacturer.
- Some extensions, such as .C, .ASM, and .BAS, indicate specific programming languages.

Many NetWare files follow the DOS naming conventions:

DOS file extensions used by NetWare	
EXE	DOS executable file
BAT	DOS executable batch file
DAT	ASCII text file (usually)
COM	DOS executable command file
ERR	Error log file
OVL	Overlay file used as part of NetWare menu utilities created from C-Worthy program to share code
HLP	Help screens which appear by pressing F1 in a menu utility
SYS	Operating system file

Other files have NetWare-specific extensions:

NetWare-specific extensions	
CFG	NetWare configuration file used to set NetWare configurations
DSK	NetWare disk driver
LAN	NetWare LAN driver
LNK	NetWare data file used by linker
PDF	NetWare printer definition file
Q	NetWare print job file
QDR	NetWare print queue definition directory
SRV	NetWare operating system file for the print queue
VAP or VP0-9	Value-Added-Process files that can be loaded at server boot

File indexing

See **FAT (Turbo FAT).**

File locking

File locking ensures that a file will be updated correctly before another user, application, or process will be allowed to write to the file.

Without file locking, one user could overwrite the file update of another user if both attempt to update the same word processing file simultaneously.

See also **Record locking.**

File rights

See **Security (Rights security).**

File scan right

See **Security (Rights security).**

File server

A computer that runs NetWare operating system software. The NetWare operating system enables the file server to regulate communications among the computers attached to it and to manage any shared resources (such as printers). The file server must have at least one hard disk, either internal or external, at least one network board, and a LAN driver to communicate with a network.

NetWare file servers are either dedicated (used as a file server only) or nondedicated (used as a file server and a workstation) and should have 2.5MB (2,560KB) of RAM. Adding VAPs (Value-Added Processes) and large or additional hard disks increases system memory requirements.

Booting the file server. Dedicated servers can boot using the cold boot loader or diskette. Nondedicated servers boot from DOS via a floppy diskette or an active DOS partition on the file server hard disk. You can set up the file server to boot automatically by placing an AUTOEXEC.BAT file on the server's boot diskette or by creating a DOS partition on the file server's DOS-addressable internal hard disk. The AUTOEXEC.BAT file executes the NET$OS.EXE file.

See also "Managing the file server" in *Using the Network*.

Bringing down the file server. Many maintenance procedures require bringing down the file server with DOWN or FCONSOLE. Changes made to data files are often held in the file server's cache memory until the file server processor has idle time. When you down the file server, the data in the cache memory is written to disk, thus preventing data loss. Users on the file server should be notified that the server is going down so that they can save their files and log out beforehand.

Related utilities: BROADCAST; DOWN; FCONSOLE (see *Using the Network*).

File server console operator

A user or a member of a group to whom SUPERVISOR delegates certain rights in managing the file server. A file server console operator has rights to use FCONSOLE with full functionality to

- Broadcast messages to users
- Change file servers
- Access connection information
- Monitor file/lock activity
- Check LAN driver configurations
- Purge all salvageable files

- Examine statistics
- Change the system date and time
- Enable or disable login for additional users
- Enable or disable the Transaction Tracking System
- View NetWare version information

See also **User (SUPERVISOR).**

Related utilities: FCONSOLE; SYSCON (see *Using the Network*).

File sharing

A feature of networking that allows more than one user to access the same file at the same time.

See also **Security (Attribute security).**

Flag

See **Security (Attribute security).**

Form

In a NetWare printer command, the name and size of the paper used for a print job.

Related utility: PRINTDEF (see *Using the Network*).

Format

See **ZTEST.**

Frame

1. A variation of a protocol, such as Ethernet II, Ethernet 802.3, Ethernet 802.2, Ethernet SNAP, Token-Ring, or Token-Ring_SNAP. See also **Ethernet configuration.**

2. A packet. See **Message packet.**

GGG

Gateway

A communication link between two networks. A gateway allows communication between dissimilar protocols (for example, NetWare and non-NetWare networks) that use industry standard protocols such as TCP/IP, X.25, or SNA.

Groups

Creating groups allows network supervisor to deal with users collectively rather than individually. When users are created, they automatically become members of the group EVERYONE and have the rights assigned to that group.

Use SYSCON to create as many as 26 groups based on who uses the same applications, printers, or print queues, who performs similar tasks, or who has similar needs for information. For example, if several users need access to files in the SALES directory, you could create a SALES group and make each of the users a member of the group.

Use SYSCON or FILER to assign group trustee rights for directories and files.

You can also use defined groups to simplify login scripts. By using groups (formed on the basis of common application use) and the conditional IF...THEN, you can map a search drive to the application directory the group needs to access. For example, if you include the following command in the system login script, you would not have to include it in the user script for each group member:

```
IF MEMBER OF "SALES" THEN
MAP *2:=SYS:SALES
```

You can also use "IF...THEN" with a groupname to EXIT to a menu created for the group, as in the following example:

```
IF MEMBER OF "SALES" THEN
EXIT TO SALES.MNU
```

Or you can prepare a login message to be displayed for group members when they log in. This line could be added to the system login script:

```
IF MEMBER OF "SALES" THEN
WRITE "Don't forget the Monday Booster Meeting!"
```

See also **Login script; User (EVERYONE).**

Related utilities: FILER; SYSCON (see *Using the Network*).

GUEST

See **User (GUEST).**

HHH

Handshaking

The initial exchange between two data communication systems prior to and during data transmission to ensure proper data transmission. A handshake method is part of the complete transmission protocol.

A serial (asynchronous) transmission protocol might include the handshake method (XON/XOFF), baud rate, parity setting, number of data bits, and number of stop bits.

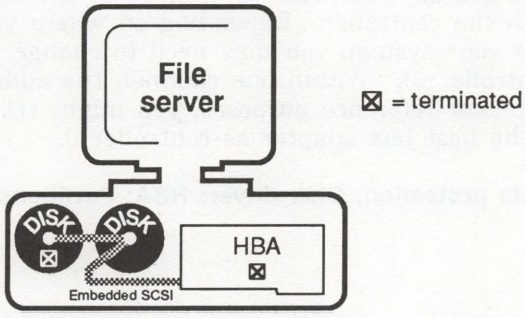
See also **Serial communication.**

Hard disk

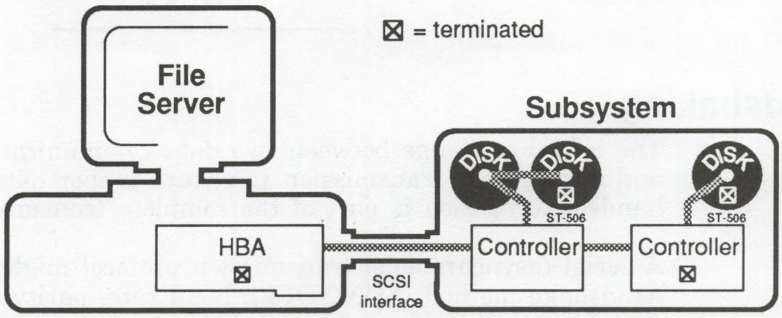
A high-capacity magnetic storage device that allows a user to write and read data; these can be network or local workstation disks. Internal disks use channel 0 and external hard disks use channels 1 through 4.

Termination. Signals to a hard disk travel along a cable or bus that is in many ways analogous to a pipe. You must terminate the end components, that is, the last controller and the last hard disk on each controller on the bus, to ensure that the data signal does not "echo" back along the bus and cause corruption. The following illustrations show which controllers and disks need termination. Since boards vary in their design, the terminator's placement depends on the board you have and whether you have internal disks, a disk subsystem, or both.

If the computer has no built-in controller on its system board and the additional hard disk controller is used to control internal hard disks only, leave the additional controller's terminators in place as follows.

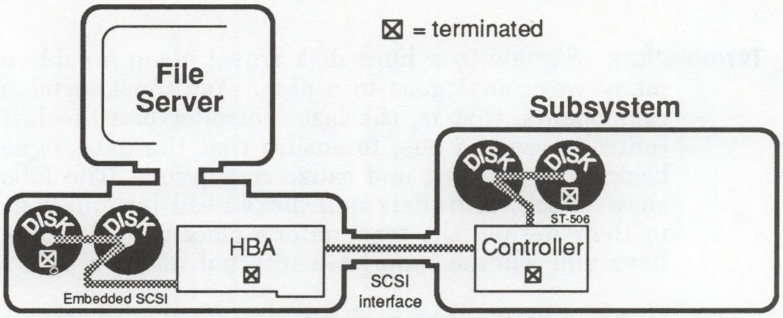


If the additional hard disk controller controls only disks in a disk subsystem, terminate the disks and controller as follows.



Terminators on the additional hard disk controller should be left in place. If you have more than one disk subsystem connected to the bus, terminate only the last controller coming off the bus.

If the additional hard disk controller is used to control both internal hard disks and disk subsystems, terminate the controllers as follows.



Addressing. Each controller must have a unique address on the disk channel. You can find the physical address settings in the documentation shipped with the controller. Depending on where you place the controller in your system, you may need to change the default setting (usually controller 0). Within one channel, the addresses can range from 0 to 7. For reference purposes, you might set the controller nearest to the host bus adapter as controller 0.

See also **Data protection; Disk driver; HBA; Partitions.**

Hardware interrupt

See **Configuration option.**

Hashing

See **Cache memory.**

HBA (Host Bus Adapter)

A board (often intelligent) that acts as an interface between the host microprocessor and the disk controller. The HBA relieves the host microprocessor of data storage and retrieval tasks, usually increasing the computer's performance time.

A host bus adapter (or host adapter) and its disk subsystems make up a disk channel. The NetWare operating system can handle up to five host adapter channels (with four controllers per channel and eight drives per controller without exceeding a total of 32 drives).

A SCSI (Small Computer System Interface) HBA is the third-party equivalent of a Novell DCB (Disk Coprocessor Board). The SCSI standard allows each host adapter a maximum of eight SCSI controllers, with each controller supporting up to two disk drives. External SCSI disk drive subsystems can be daisy-chained off the host adapter port.

File servers with ISA (AT bus) or EISA architecture use HBAs.

See also **Hard disk; SCSI bus.**

Hexadecimal

A base-16 numeric notation system frequently used to specify addresses in computer memory. In hexadecimal notation, the decimal numbers 0 through 15 are represented by the decimal digits 0 through 9 and the alphabetic "digits" A through F (A=decimal 10, B=decimal 11, and so forth).

Hidden attribute

See **Security (Attribute security).**

Home directory

A private network directory that the network supervisor can create for a user. The user's login script should contain a drive mapping to his or her home directory.

Host bus adapter

See **HBA.**

Hot Fix

See **Data protection.**

Hub

A device that modifies transmission signals, allowing the network to be lengthened or expanded with additional workstations.

See also **Active hub; Passive hub.**

III

Identifier variables

See **Login script.**

Indexed attribute

See **Security (Attribute security).**

Initialize hard disk

See **ZTEST.**

Interleave

(Interleave factor) A method of adjusting the speed of the controller to match the speed of the hard disk. Typically, a hard disk spins faster than a controller can perform a read/write request. If the controller is not fast enough to read or write consecutive sectors on a hard disk track, then the controller can be programmed to skip one or more sectors before the next read/write request is performed.

If the controller reads or writes one sector and then skips a sector, the interleave is 2 (every other sector is used to store logically consecutive blocks). The interleave is sometimes written as 2:1. If the controller writes to one sector and then skips two, the interleave is 3 or 3:1.

The interleave factor is usually established by the manufacturer or reseller of the hard disk/controller combination. If someone else assembles the hard disk/controller combination, he or she may need to experiment to determine the correct interleave factor.

Internal router

See **Router.**

Internetwork

Two or more networks connected by an internal or external router. Users on an internetwork can use the resources (such as files, printers, or hard disks) of all connected networks, provided they have the appropriate security clearance.

See also **Router; Security.**

Interrupt

See **Configuration option.**

Intruder detection

See **Security (Account restrictions).**

I/O address

See **Configuration option.**

IPX.COM

See **NetWare workstation files (IPX.COM).**

IPX drivers

IPX drivers are IPX.COM files created with WSGEN. These drivers work only with the IPX/SPX protocol.

See also **NetWare workstation files.**

IPX/SPX protocol

See **NetWare workstation files (IPX.COM).**

IRQ

See **Configuration option.**

Isolation transformer

See **Power conditioning.**

JJJ

Jumper block

A group of pins which can be connected (jumpered) or left unconnected to make hardware configuration settings on a printed circuit board.

LLL

LAN board

See **Network board.**

LAN driver

See **NetWare workstation files.**

Line-surge suppressor

See **Power conditioning.**

Log in

A procedure that provides access to the network by initializing a user's security rights and environment. When a user initiates a login request, the operating system scans the file server's bindery and reads the user's bindery information into memory. The user may then be asked for a password.

The appropriate security information is then placed in the file server's connection list and the user is said to be "logged in." At this point, LOGIN executes the login script.

See also **Bindery; Login script;** "Logging in and out" in *Using the Network.*

Log out

Breaking the file server/workstation connection and deleting any drives mapped to the file server, using LOGOUT. If you are connected to several file servers and log out without specifying a file server name in the LOGOUT command, the workstation connections and mapped drives to all file servers will be terminated.

If you maintain connection with at least one file server, make sure that one of the remaining drives is mapped to the PUBLIC directory of a file server that you are still attached to. Otherwise, you will not be able to access any NetWare utilities. If you cannot access the NetWare utilities, you can use DOS CD to find the PUBLIC directory and map new drives from there. It may be easier to just log in to the file server again and allow your login script to set drive mappings.

See also "Logging in and out" in *Using the Network*.

Related utilities: LOGIN; LOGOUT; SYSCON (see *Using the Network*).

LOGIN directory

(SYS:LOGIN) A system-created directory that is created automatically during network installation and cannot be deleted. LOGIN and SLIST are copied into the LOGIN directory. Users can log in to the network and view a list of available network servers from this directory.

Login restrictions

Login restrictions control individual user accounts; most restrictions can also be set on a system-wide basis. When login requirements are not met (a password has expired or a user attempts to log in during a restricted time), NetWare disables the user account. This makes it difficult for unauthorized users to log in to the file server. NetWare employs the following restrictions.

Account balance restrictions. If you have installed Accounting to regulate network resources, you can assign initial account limits for users. When the account is depleted, NetWare disables the account.

Expiration restrictions. You can specify an expiration date for a user account. The account expires at 12:01 a.m. the next day.

Password restrictions. You determine whether to require passwords. If you require passwords, you can also specify the minimum length of passwords, how often the password must be changed, whether the password must be unique (different from the previous eight passwords used by the account), and whether the user can change the password. If you allow users to change passwords, they can also edit their own login scripts.

You can also specify the number of times a user can log in with an expired password (grace logins) or the number of incorrect login attempts. When that number is exceeded, the account is disabled. Incorrect attempts only temporarily disable logins.

Disk space restrictions. If the "Limit Disk Space" parameter was set during installation, you can limit the maximum number of blocks available to each user.

Connection restrictions. You can limit the number of workstations a user can log in from concurrently or specify which workstation(s) a particular user can use.

Time restrictions. You can restrict the hours during which users can log in. You can restrict all users to the same hours or restrict users individually.

Login script

A login script contains commands that initialize environmental variables, map network drives, or control the user's program execution upon logging in. Login scripts are similar to configurable batch files and are executed as part of the login procedure.

NetWare features three types of login scripts: a default script, a system script, and a user script.

A **default login script** is executed if no system or user login script exists. This is the same login script you see when you log in to the file server as SUPERVISOR for the first time. The code for the default login script is contained in the LOGIN.EXE file in SYS:LOGIN and cannot be edited. The default login script is coded as follows.

```
WRITE "Good %GREETING_TIME, %LOGIN_NAME."
MAP DISPLAY OFF
MAP ERRORS OFF
Remark: Set 1st drive to most appropriate directory.
MAP *1:=SYS:;*1:=SYS:%LOGIN_NAME
If "%1"="SUPERVISOR" THEN MAP *1:SYS:SYSTEM
Remark: Set search drives  (S2 machine-OS dependent).
MAP S1:=SYS:PUBLIC; S2:=S1:%MACHINE/%OS/%OS_VERSION
Remark: Now display all the current drive settings.
MAP DISPLAY ON
MAP
```

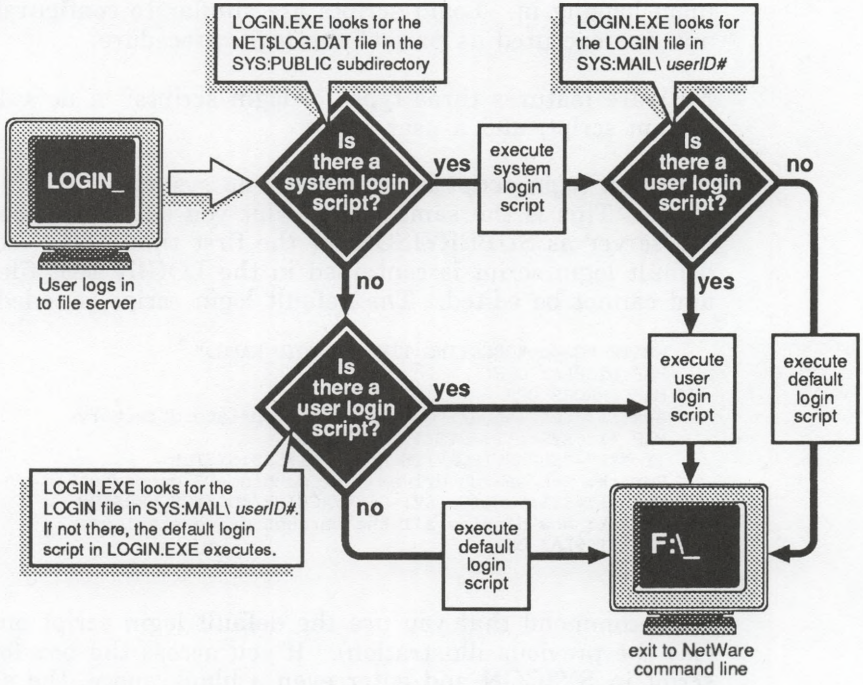
We recommend that you use the default login script only temporarily (see the previous illustration). If you access the box for a user login script in SYSCON and enter even a blank space, the system considers a user login script to exist and prevents the user from accessing the default login script when logging in.

The **system login script** is created by the network supervisor. It should include any network drive mappings, search drive mappings, and any commands that should be executed for every user or for defined groups of users. Because the system script is created in SYSCON and stored in a general access directory, no passwords or proprietary information should be included in the system login script.

A **user login script** executes after the system login script and should include drive mappings and environment variables that are specific to the particular user. A user login script is created and modified using SYSCON. Users who are allowed to change their own passwords can create and modify their own scripts. We recommend that you create a system login script before you create user login scripts.

A backup file, LOGIN.BAK, is created in each user's ID subdirectory when the login script is modified; this file can be renamed LOGIN if you ever delete or write over the original LOGIN by mistake.

After a user initiates a login request and supplies the correct username and password, LOGIN executes login script commands as illustrated in the following figure.


LOGIN.EXE looks for the NET$LOG.DAT file in the SYS:PUBLIC subdirectory
LOGIN.EXE looks for the LOGIN file in SYS:MAIL\ userID#
LOGIN_
User logs in to file server
Is there a system login script?
yes
execute system login script
Is there a user login script?
no
yes
no
Is there a user login script?
yes
execute user login script
execute default login script
LOGIN.EXE looks for the LOGIN file in SYS:MAIL\ userID#. If not there, the default login script in LOGIN.EXE executes.
no
execute default login script
F:_
exit to NetWare command line

Login script conventions. Login script commands must be entered following the command format conventions described in "Logging in and out" in *Using the Network*. The command format specifies the proper syntax for keywords, variables, parameters, spacing, delimiters, or other characters and punctuation.

What should a system login script provide? We recommend including as much as possible in the system login script. The more a system login script accomplishes, the shorter user login scripts can be.

Some commands are essential in a login script, some are recommended, and others are optional or dependent on the needs of your network users.

Login script commands are described individually in *Using the Network*.

Essential commands provide access to NetWare and DOS.

- NetWare utilities

  Use MAP or MAP INSERT to map the first search drive to SYS:PUBLIC. This mapping provides access to NetWare utilities (and any application or batch files you want to store in a public access directory) from any directory.

  ```
  MAP S1:=SYS:PUBLIC
  ```

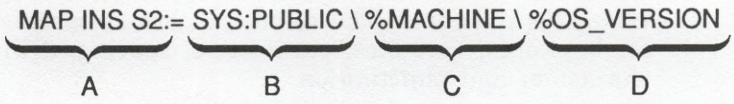
- DOS commands

  Use MAP or MAP INSERT to map the second search drive to the directories that store the DOS files and utilities you are using on the network. You can include search drive mappings in the system login script that use shell identifiers to give each workstation access to the appropriate version of DOS.

  The search drive can consist of one or two variables that identify the DOS version used on the workstation, the machine type (%MACHINE) and/or DOS version (%OS_VERSION). The variables use the default parameters set in the network shell running on each workstation. The default parameters can be altered by defining a SHELL.CFG file on the workstation boot diskette.

See also "Managing DOS workstations" in *Using the Network*.

The format for mapping the search drive should resemble this:



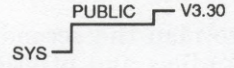
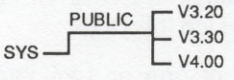
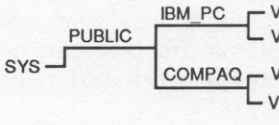
A: Places the search drive with priority just after SYS:PUBLIC.

B: Looks for the files in a directory under SYS:PUBLIC.

C: Generic identifier variable that makes the search specific to the directory for the type of machine the workstation uses. The default value is IBM_PC. If another type of machine is used, insert the LONG MACHINE TYPE statement into the SHELL.CFG file (for example, `long machine type=compaq`).

D: Generic identifier variable that makes the search specific to the directory corresponding to the workstation's DOS version. The value is determined by the version of DOS the workstation is booted with.

The format of the search drive must reflect the directory structure that contains the DOS files, as in the following examples:

Directory structure	Search drive mappings
Example 1—*Workstations with the same machine types and DOS versions* 	**MAP INS S2:= SYS:PUBLIC\V3.30**
Example 2—*Workstations with the same machine types and different DOS versions* 	**MAP INS S2:= SYS:PUBLIC\%OS_VERSION**
Example 3—*Workstations with different machine types and different DOS versions* 	**MAP INS S2:= SYS:PUBLIC\%MACHINE\%OS_VERSION**

Note: The default login script requires an additional level, %OS. If you use the default login script, you must create a directory structure to match PUBLIC\%MACHINE\%OS\%OS_VERSION, such as PUBLIC\IBM_PC\PC_DOS\V3.30.

See also **Directory structure.**

Related utilities: FILER; USERDEF (see *Using the Network*).

Recommended commands provide access to frequently used directories: application, home, and work directories, for example. Use MAP to give users access to the directories they use most.

To let users know where they are in the directory structure, we also recommend that you include the [DOS] SET command to set the prompt to display the current directory path:

```
SET PROMPT="$P$G"
```

Optional commands can include or provide for displaying messages, setting environmental variables, exiting to login script batch files, attaching to additional file servers, etc. For instance, you may want to set the COMSPEC environment variable to a network drive so that COMMAND.COM reloads from the network instead of reloading from a local drive.

Using identifier variables in login scripts. Indentifier variables (for the day/month/year, the hour of the day, the station number, etc.) are useful in WRITE commands, IF...THEN conditionals, and commands for which you can specify a pathname. For example, a user script could include the following:

```
WRITE "%HOUR: %MINUTE: %SECOND"
```

When the user logs in, the correct text will be substituted for the identifier variables (HOUR, MINUTE, and SECOND) and displayed on the screen.

Variables must be entered in uppercase and be preceded by a percent sign. If they are embedded in WRITE commands, the text string must be enclosed in quotation marks (as in the example above).

Refer to the chart on the next page for an explanation of identifier variables.

For further information about identifier variables and other login script commands, see "Logging in and out" in *Using the Network*.

	Identifier variable	Description
Conditional	ACCESS_SERVER	Returns TRUE if Access Server is Functional, otherwise FALSE
	ERROR_LEVEL	An Error Number, 0=No Errors
	MEMBER OF *"group"*	Returns TRUE if member of group, otherwise FALSE
Date	DAY	Day number (01-31)
	DAY_OF_WEEK	Day of week (Monday, Tuesday, etc.)
	MONTH	Month number (01-12)
	MONTH_NAME	Month name (January, June, etc.)
	NDAY_OF_WEEK	Weekday number (1-7, Sunday=1)
	SHORT_YEAR	Year in short format (88, 89, etc.)
	YEAR	Year in full format (1988, 1989)
DOS Environment	< >	Use any DOS environment variable as a string
Network	NETWORK_ADDRESS	Network number of the cabling system (8 hex digits)
	FILE_SERVER	Name of the file server
Time	AM_PM	Day or night (am or pm)
	GREETING_TIME	Morning, afternoon, or evening
	HOUR	Hour of day or night (1-12)
	HOUR24	Hour (00-23, midnight = 00)
	MINUTE	Minute (00-59)
	SECOND	Second (00-59)
User	FULL_NAME	User's full name (from SYSCON files)
	LOGIN_NAME	User's unique login name
	USER_ID	Number assigned to each user
Workstation	MACHINE	The machine the shell was written for, e.g., IBMPC
	OS	The workstation's operating system, e.g., MSDOS
	OS_VERSION	The version of the workstation's DOS
	P_STATION	Station number or node address (12 hex digits)
	SMACHINE	Short machine name, e.g., IBM
	STATION	Connection number

Long machine type

A six-letter name representing a workstation brand. Use the long machine type as a variable in system login scripts (%MACHINE) to map a drive to the version of DOS assigned to a workstation (the DOS directory must have the same name as the long machine type). The name is set in the SHELL.CFG file. The default is IBM_PC. If the workstation is not an IBM computer, you must create a long machine type for the workstation in SHELL.CFG.

See also **Directory structure; DOS version; Login script.**

LPT1

The primary parallel printer port of a personal computer. See also **Parallel port.**

MMM

MAIL directory

A directory created automatically during network installation. When network users are created, they are assigned a User ID number. (The supervisor is always given ID number 1; other users are randomly assigned unique numbers by the file server.) Users are also assigned a subdirectory, or mailbox, in the MAIL directory. The User ID number is used as the mailbox name.

Users are given all rights except Access control in their mailboxes and only the Create right in the MAIL directory to allow users to deliver messages (drop off files) to other users. Each user's login script is stored in his or her mailbox, allowing the login script to be accessed each time the user logs in.

Map or Mapping

To assign a drive letter to a chosen directory path on a particular volume of a particular file server. For example, if you map drive F to the directory SYS:ACCTS\RECEIVE, you will access that directory every time you enter "F:" at the DOS prompt.

See also **Directory structure; Drive mappings; Login script.**

Master workstation diskette

A master workstation diskette is used to simplify the process of installing numerous workstations on a network. When you create the IPX.COM file with WSGEN, you can place it and NET*x*.COM on a master workstation diskette. Make copies of this master for each workstation that needs the files for booting (i.e., any workstation that has the same type of network board, configuration option, and DOS version).

When you use a master workstation diskette, you save the time it would take to run WSGEN.EXE for each workstation with identical boot file requirements.

See also **Boot files;** "Managing DOS workstations" in *Using the Network.*

Maximum Rights Mask

See **Security (Rights security).**

Memory board

An add-on board designed to increase a computer's amount of RAM.

MENU

NetWare allows you to create and access customized menus using the MENU command line utility. You can create your own menus using a text editor, specifying the applications or commands to be included, the placement of the menu on the screen, and the color palette to be used.

What the menu contains is determined by what applications or commands a user needs, and the user's level of expertise with DOS, NetWare, and the application that he or she uses. A separate menu can be created for each user if necessary.

For example, you may want to create a menu listing the two or three applications that the user will access on a regular basis, plus one or two NetWare or DOS commands. If the user uses several applications, you can group the applications in submenus. For example, you could have a submenu for word processing applications, another for database applications, and another for utilities and miscellaneous commands.

The commands for creating a menu are placed in a text file. To start the menu, include a line in the user's login script or enter the MENU command at the command line. For example, if the name of the menu text file for user Fred is FREDMENU.MNU, you would place the following line at the end of Fred's login script so that the menu appeared automatically when Fred logged in:

```
#MENU FREDMENU.MNU
```

Or, Fred could also type the following command at the command line each time he logs in:

```
MENU FREDMENU.MNU <Enter>
```

If the filename has the extension .MNU, you do not need to enter the extension. If the filename has any other extension, you will need to specify it.

Screen position. The position of the menu on the screen is specified by the number of lines down and the number of characters over from the top-left corner of the screen. The numbers count to the center of the menu. Suppose Fred's menu is positioned at 10,20. This means that the center of the menu is 10 lines down from the top of the screen and 20 characters to the right of the left edge of the screen.

To calculate a screen position for the menu, you must determine the height and width of the menu that you are creating, sketch out the menu, then count the lines and characters in the menu. Suppose Fred's menu contains 6 lines, and the longest line contains 18 characters.

To position the menu 5 lines down from the top of the screen, you would enter a value of 8 (or 5 for the lines above the menu and 3 from the top of the menu to its center).

To position the menu 20 characters from the left of the screen, you would enter a value of 29 (or 20 for the characters to the left and 9 from the left side of the menu to its center).

Color palette. The color palette for a menu specifies which colors will be used for the background and foreground (text). Five color palettes are defined by NetWare during installation; you can use one of these palettes or create additional palettes for your own use. Palette numbers 0 through 4 specify the NetWare palettes.

See also "Customizing network menus" in *Using the Network.*

Related utilities: COLORPAL; MENU (see *Using the Network*).

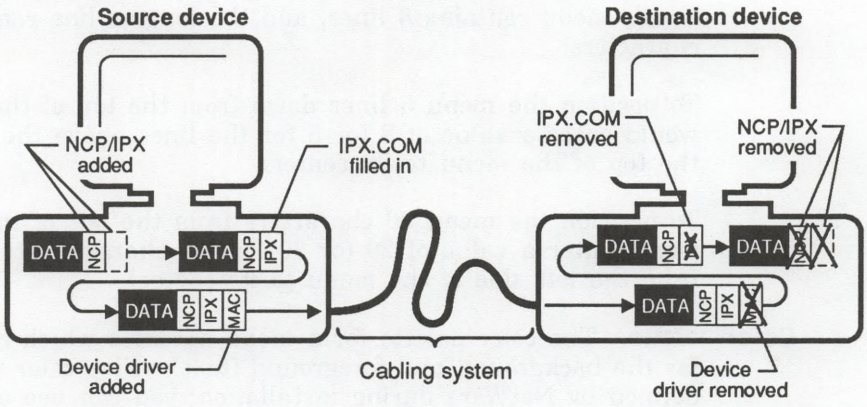
Message packet

A unit of information used in network communication. Messages sent between network devices (workstations, file servers, etc.) are formed into packets at the source device. The packets are reassembled, if necessary, into complete messages when they reach their destination. A message packet might contain a request for service, information on how to handle the request, and the data that will be serviced.

An individual packet consists of headers and a data portion. Additional headers are appended to the data portion as the packet travels through the layers of the communication protocol. Any message that exceeds the maximum size is partitioned and carried as several packets. When the packet arrives at its destination, the headers are stripped off in reverse order and the request is serviced.

For example, the NetWare Core Protocol (NCP) attaches a write request header and an IPX header to a piece of data to be written. Then the workstation's IPX/SPX communication protocol fills in the IPX header, designating, among other things, the source of the request and the packet length. Finally, the device driver adds a hardware or MAC (Media Access Control) header.

The following illustration shows a message packet traveling from a source device to a destination device.



See also **Communication protocols; NCP services.**

Message system

A communication protocol that runs on top of IPX/SPX. It provides an engine that allows a node on the network to send messages to other nodes in an MHS (Mail Handling System). A set of APIs (Application Program Interfaces) gives programs access to the message system. NetWare v2.2 supports file server broadcasts and alerts to supervisors and Workgroup Managers.

Mirroring

See **Disk mirroring.**

Modify right

See **Security (Rights security).**

Multiple file server network

See **Multiserver network.**

Multiple-byte character

Refers to characters made up of more than one byte. The ASCII character set defines a maximum of 256 characters. A computer handles each ASCII character with one byte. Because Asian character sets require more than 256 characters, a computer must use two bytes (double bytes) for each character. NetWare does not support multiple-byte characters.

Multiserver network

A single network (one cabling system) that has two or more file servers attached. Network addresses assigned to the LAN drivers are the same in each file server because the network boards are attached to the same cabling system. On a multiserver network, users can access files from any file server to which they are attached (if they have access rights). A multiserver network should not be confused with an internetwork (two or more networks linked together through an internal or external router).

See also **Network address.**

NNN

NCP (NetWare Core Protocol) services

Procedures that a file server's operating system follows to accept and respond to workstation requests.

The process of requesting service from a file server begins in the workstation's RAM where the NetWare shell (NET*x*.COM) forms requests according to the definitions of the file server's NetWare Core Protocol (NCP). The shell then hands the requests to the workstation's IPX/SPX communication protocol. IPX transmits the request to the file server after attaching a header designating the source and destination. Upon receiving the request, the file server strips off the IPX header and reads the request. Because the NetWare shell has formed the request using the exact guidelines of a specific service protocol, the file server handles the request according to the protocol rules, resulting in a proper response.

NCP services exist for every service a workstation can request from a file server. Common requests include creating or destroying a service connection, manipulating directories and files, opening semaphores, altering the bindery (drive mappings and security), and printing.

See also **Communication protocols; NetWare workstation files.**

NetBIOS emulator

An emulator program provided with NetWare that allows workstations to run applications that support IBM's NetBIOS calls.

NET*x*.COM

See **NetWare workstation files.**

NetWare Core Protocol

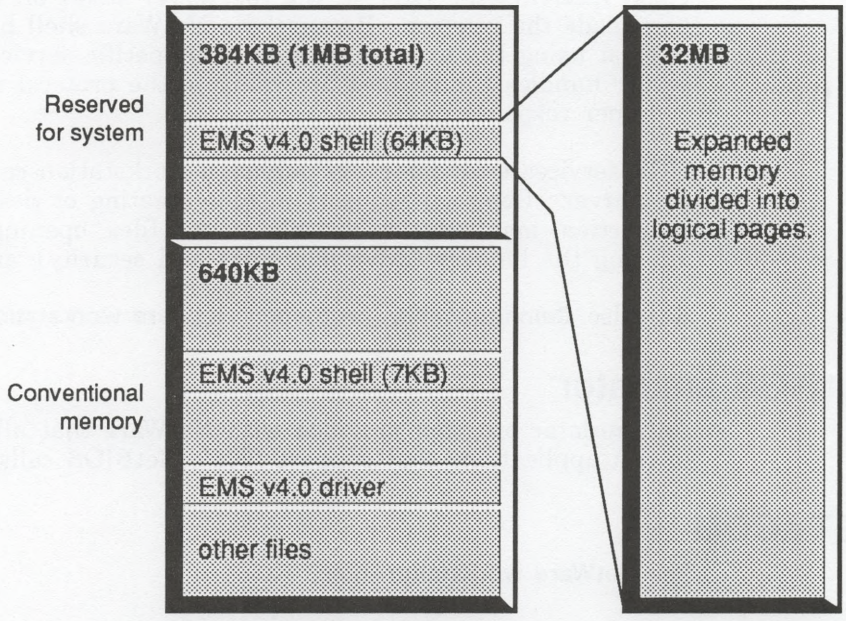
See **NCP services.**

NetWare expanded memory shell

Refers to memory in addition to the 640KB limit of conventional memory. An expanded memory manager swaps memory that exists above the 1MB range into a window, or memory page, below the 1MB range. This allows DOS applications to access up to 32MB of expanded memory.

The NetWare expanded memory shell moves most of the shell out of conventional DOS memory and puts it in expanded memory. This frees up about 33KB of memory. At least 7KB of the shell must remain in conventional memory. It contains data and code to handle interrupts.

The NetWare expanded memory shell was written to LIM/EMS (Lotus/Intel/Microsoft/Expanded Memory Specification) v4.0 memory manager specifications.



Expanded memory shell

Expanded memory board manufacturers provide EMS (Expanded Memory Specification)-compatible drivers. You must load an EMS-compatible driver before loading the NetWare expanded memory shell.

To install the NetWare expanded memory shell, you need to

- Load a third-party EMS-compatible driver
- Copy the EMSNET*x*.EXE file to the workstation boot diskette
- Include the filename EMSNET*x*.EXE in the AUTOEXEC.BAT file

Because the expanded memory shell operates in expanded memory, larger applications can run in the conventional memory space. This approach is faster than disk swapping and overlays.

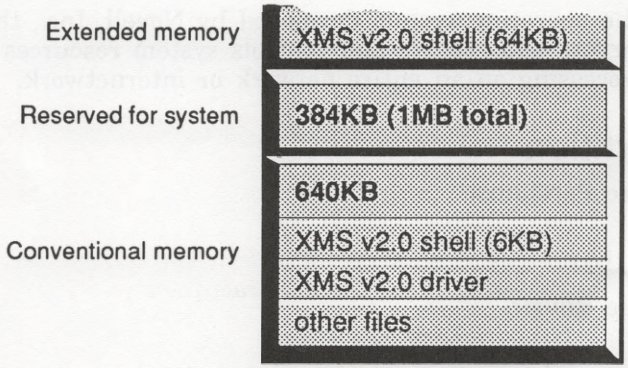
The NetWare expanded memory shell works with NetWare v2.1 and above. All shell configuration (SHELL.CFG) parameters work with the NetWare expanded memory shell.

EMSNET*x*.EXE can be used only with DOS 3.0 and above. The expanded memory shell is not designed to work on a computer running nondedicated NetWare.

NetWare extended memory shell

Moves most of the shell out of conventional DOS memory into addressable memory above the 1MB range, freeing up 34KB of conventional memory. At least 6KB of the shell must remain in conventional memory. It contains data and code to handle interrupts.

The extended memory shell requires the support of an XMS (e**X**tended **M**emory **S**pecification) v2.0 memory manager (or compatible) such as Microsoft's HIMEM.SYS. The memory manager makes the first 64KB (beginning at the 1MB address) of extended memory directly available to DOS-based applications.



Extended memory shell

To install the NetWare extended memory shell, you need to

- Load a third-party extended memory manager
- Copy the NetWare extended memory shell, XMSNET*x*.EXE, to the workstation boot disk
- Include the filename XMSNET*x*.EXE in the AUTOEXEC.BAT file (*x* represents the version of DOS you are using)

Because the Extended memory shell operates in extended memory, larger applications can run in the conventional memory space. This approach is faster than disk swapping and overlays.

The NetWare extended memory shell works with all versions of NetWare v2.1*x* and above.

All the shell configuration (SHELL.CFG) parameters work with the NetWare extended memory shell.

XMSNET*x*.EXE can be used only with DOS 3.0 and above. The current VDISK.SYS from IBM is not compatible with HIMEM.SYS, so the extended memory shell can't be used with VDISK.SYS. The extended memory shell is not designed to run on a computer running nondedicated NetWare.

This shell requires a high degree of IBM compatibility. Depending on the brand of IBM compatible you are using, you may experience keyboard sluggishness or other hardware problems.

See also **Boot files.**

NetWare operating system

The operating system developed by Novell, Inc., that runs in file servers and routers and controls system resources and information processing on an entire network or internetwork.

NetWare partition

See **Partitions.**

NetWare router

See **Router.**

NetWare workstation files

Files that, along with a network board, convert a standalone computer into a network workstation. These files are memory-resident programs—IPX.COM (a protocol/LAN driver file) and NET*x*.COM (the NetWare shell).

When a DOS workstation is booted, NET*x*.COM loads the NetWare shell into the workstation's RAM as a TSR (Terminate-and-Stay Resident) program that provides an interface between the application and DOS. The shell intercepts application requests and determines whether to route them locally to DOS or to the network file server for service by the NetWare operating system using NCP (NetWare Core Protocol). If the request needs services from the network, the shell makes any necessary protocol conversions.

Although NET*x*.COM is the actual NetWare shell, it is closely linked to other programs and routines to achieve necessary network communications. The shell uses the protocol program to assign source and destination addresses to a data packet. The default NetWare protocol is IPX/SPX, which uses a LAN driver to control transmissions through the network board.

IPX.COM is generated when you run WSGEN (WorkStation GENeration) during workstation installation. WSGEN links (adapts) IPX to a board-specific LAN driver and a unique configuration option. The installer must copy IPX.COM and NET*x*.COM to the workstation boot disk or diskette. We recommend using an AUTOEXEC.BAT file to load these files into RAM each time the station is booted.

Most function calls send a single packet to the file server, but some calls only provide or manipulate information in the shell's own local tables. The shell initializes these tables to formulate and track NCP requests. The shell also builds a table to track connections with one or more file servers (the shell can maintain connections with up to eight file servers at once). Another set of tables keeps track of network drives and their mappings, including which file server each network drive refers to.

NET*x*.COM. This NetWare workstation shell file provides an interface between the application and DOS, monitoring all data transmissions that move in or out of either one. When a function request needs network service, such as a call to read a file from the file server, the shell begins the process of protocol conversion and network transmission.

NET*x* intercepts requests by taking over software interrupts 21h (used to call standard DOS functions), 24h (DOS's critical error handler vector), and 17h (used to send data to local printer ports). In general, the shell intercepts all interrupt 21h DOS requests and inspects each one.

After inspection, the shell either passes the request on to the regular DOS interrupt routine, or keeps it, converts the request into the corresponding NCP request, and hands it to IPX/SPX for transmission to the file server. Data returning from the file server is converted back. Request handling is totally transparent to the application and, therefore, to the user.

The following chart shows the variety of shell files available. If a workstation has expanded or extended memory, using the appropriate shell file frees up additional base memory.

DOS version	Available NetWare shell files		
	Base memory	Expanded memory	Extended memory
2.*x*	NET2. COM		
3.*x*	NET3. COM	EMSNET3.EXE	XMSNET3.EXE
4.*x*	NET4. COM	EMSNET4.EXE	XMSNET4.EXE

IPX.COM. The Novell IPX/SPX (**I**nternetwork **P**acket e**X**change/**S**equenced **P**acket e**X**change) communication protocol that creates, maintains, and terminates connections between network devices (workstations, file servers, routers, etc.). NET*x* intercepts and prepares requests (in a form understandable to the destination after network transmission). Before NET*x* hands them to IPX/SPX, IPX.COM uses a LAN driver routine to control the station's network board and address and to route outgoing data packets for delivery on the network. IPX/SPX reads the assigned addresses of returning data and directs the data to the proper area within a workstation's shell or the file server's operating system.

SPX monitors network transmissions to ensure correct delivery. If an acknowledgement request brings no response within a specified time, SPX retransmits it. After a reasonable number of retransmissions fail to return a positive acknowledgement, SPX assumes the connection has failed and warns the user of the failure.

Note: OS/2 workstations use IPX.SYS and SPX.SYS instead of IPX.COM. You can save memory by loading only IPX if you do not need deliveries guaranteed with SPX.

You can adapt IPX.COM to many different network boards. As a result, IPX.COM can route and accept data packets through physically different networks and workstations.

LAN driver. Every transmission prepared by the NetWare shell must eventually pass through the network board connecting the workstation to the network. The LAN driver makes the actual connection between the physical network board and the logical routines and programs that use it. The LAN driver is designed and configured to each network board's physical construction as well as the instructions which direct that board to transmit on the network.

A LAN driver is linked both to the specific network board and its configuration. Through the LAN driver, IPX/SPX transmits requests regardless of the type of board. In effect, different drivers allow the same operating system to use many different kinds of boards. This gives an installer great flexibility in choosing the most effective network topology.

Note: NetWare uses two types of driver protocol files. If you decide to use IPX/SPX with the LAN driver when you run WSGEN, the workstation needs only IPX.COM and NET*x*.COM. If you select DOS ODI drivers, the workstation needs the linking file LSL.COM, a driver file such as NE2000.COM, and a separate protocol file, IPXODI.COM.

See also **Boot files; Communication protocols; Configuration option; Message packet; NCP services; NetWare expanded memory shell; NetWare extended memory shell.**

NetWire

Novell's on-line information service available through CompuServe Information Service. NetWire provides access to Novell product information, Novell services information, and time-sensitive technical information for all NetWare users. NetWire allows you to

- Remotely access information 24 hours a day
- Submit questions to a Novell Technician or System Operator
- Download files and technical information dealing with product updates and modifications

NetWire requires a PC or compatible workstation, a modem, a communications program, and a subscription.

For more information about NetWire subscriptions, contact CompuServe at 1-(800)-848-8199 and ask for representative number 58. You will receive a free introductory membership to NetWire. Outside of the United States or Canada, call 1-(614)-457-0802.

Network

A group of computers on a single cabling system (identified by a unique network address) that can communicate with each other, share peripherals (such as hard disks and printers), and access remote hosts or other networks. A NetWare network consists of workstations, peripherals and one or more file servers (each identified by unique node numbers). NetWare network users can share the same data and application files, send messages between individual workstations, and protect files with an extensive security system.

Network address

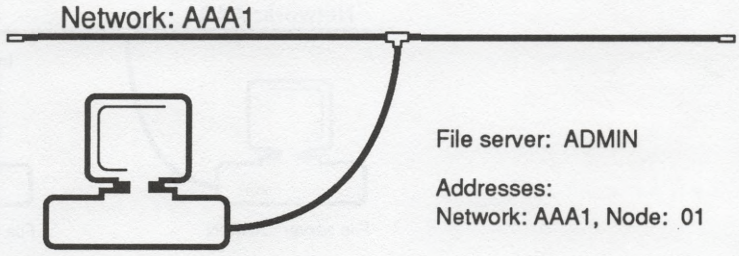
An eight-digit hexadecimal number that uniquely identifies a network. The figures on the following pages use simple network configurations to illustrate the concepts of network addressing. The network addresses used are arbitrary; any combination of hexadecimal numbers in the range of 1 to FFFFFFFE are valid network addresses. For simplicity, the illustrations use a bus topology; however, the concepts presented apply to any network topology.

Network addressing concepts can be compared to a postal numbering system. A street number or name identifies a city street, and building numbers identify individual buildings along the street. The combination of a street number or name and a building number tells the post office where to deliver mail within a city.

A network address identifies a single network cabling system. It is specified by the installer during file server or router operating system installation. Node numbers identify individual stations along the network cable and can be set in a variety of ways, depending on which network board you use: (1) with jumpers or switches on boards such as Arcnet, (2) at the factory for Token-Ring and Ethernet network boards, or (3) with software, such as the IBM *REFERENCE* diskette.

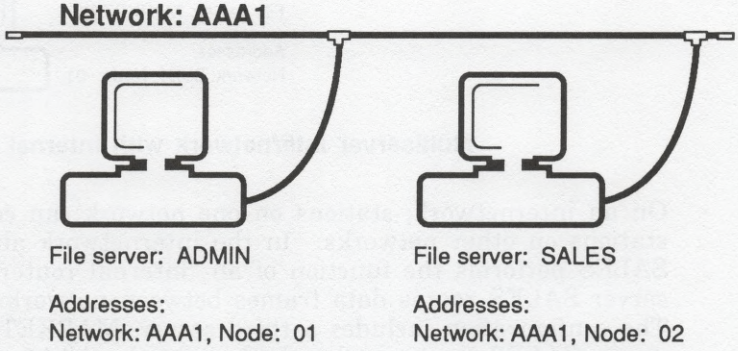
Network addresses, in combination with node numbers, allow data to be delivered to the right destination. Data is distributed on a network in envelopes called "frames." Each frame is stamped with a source and a destination address. Both the source and destination addresses consist of a network address and a node number.

Single server network. The figure below shows a simple network configuration: one server attached to one cabling system. In this configuration, the network address AAA1 identifies the network to which the server ADMIN is attached.



Single server network

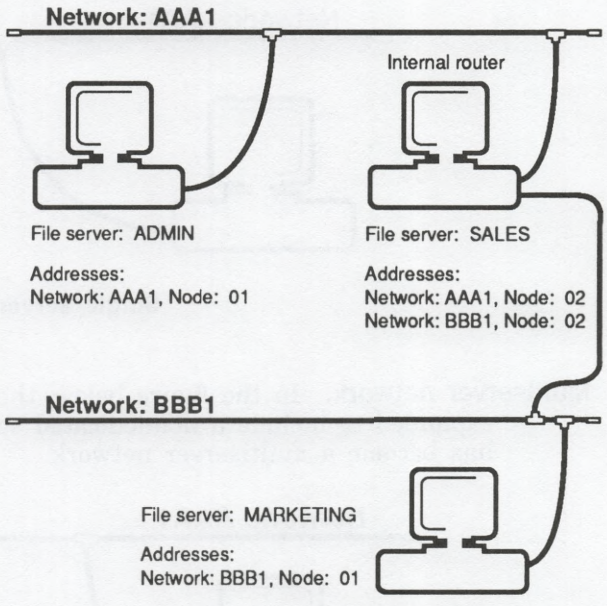
Multiserver network. In the figure below, the first configuration has been expanded to include a nondedicated server (SALES) and, as a result, has become a multiserver network.



Multiserver network

Because SALES and ADMIN share the same cabling system (network), they share the same physical network address: AAA1. However, because node numbers must be unique within each network, each server uses a different node number on network AAA1.

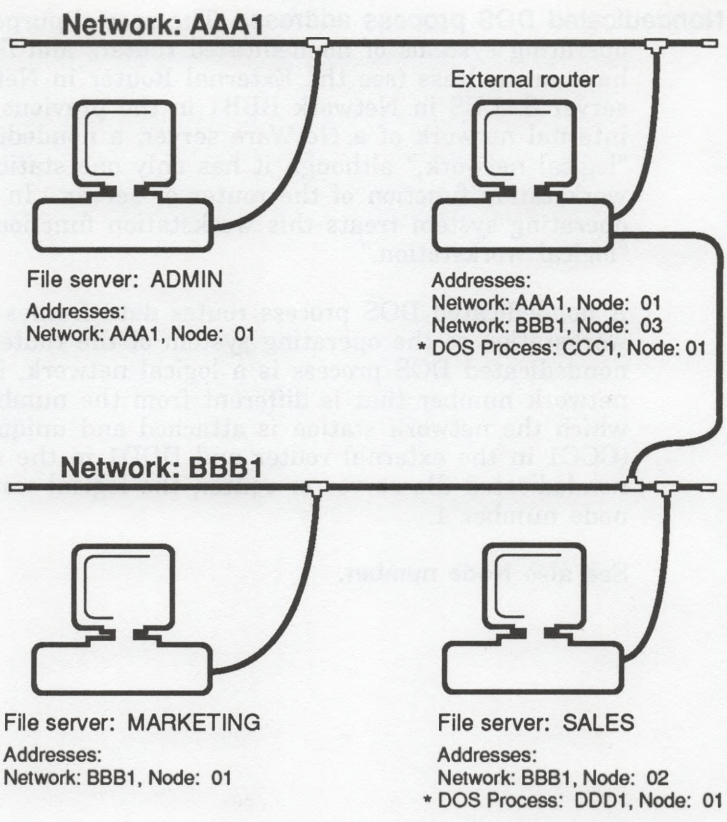
Multiserver internetwork. A second cabling system, or network, has been added to the configuration below, resulting in a multiserver internetwork. An internetwork is a series of two or more networks that are linked via internal or external routers.



Multiserver internetwork with internal router

On an internetwork, stations on one network can communicate with stations on other networks. In the internetwork above, the server SALES performs the function of an "internal router." This means that server SALES routes data frames between networks AAA1 and BBB1. The configuration includes a third server, MARKETING. Because server SALES is attached to both networks AAA1 and BBB1, all three servers can communicate with each other.

Multiserver internetwork. The following figure expands the configuration with a second network. This is a multiserver internetwork that uses an external router between the networks AAA1 and BBB1. An internetwork is a series of two or more networks that are linked via internal or external routers.



* Used with nondedicated file servers and routers

Multiserver internetwork with external router

The external router performs the same functions as server SALES in the previous figure, routing services between the networks AAA1 and BBB1. Server SALES in the above figure is relieved from the task of routing data frames between different networks. However, now SALES and the router also serve as workstations with unique addresses.

The configuration above also includes server MARKETING. Because server MARKETING is attached to the network BBB1, the router of server MARKETING must use the network number BBB1 and a node number that is unique on network BBB1.

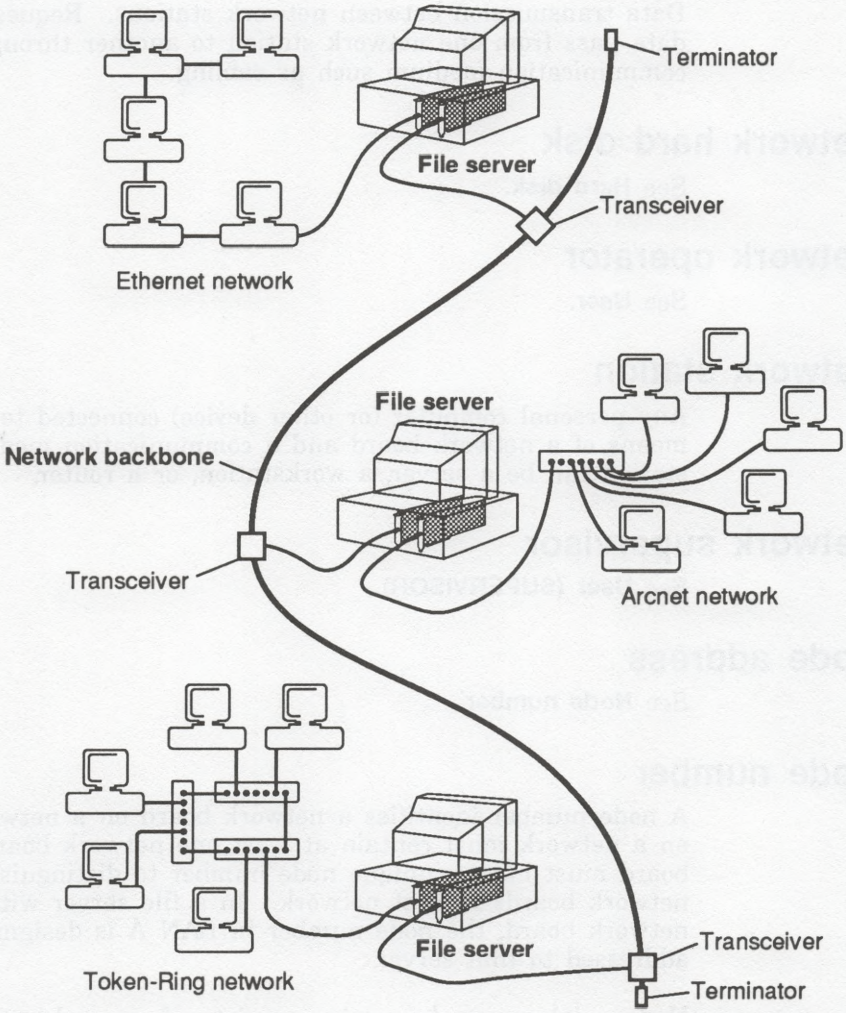
Nondedicated DOS process address. The special-purpose router used in the operating systems of nondedicated routers and file servers must also have an address (see the External Router in Network AAA1 and the server SALES in Network BBB1 in the previous illustration). Like the internal network of a NetWare server, a nondedicated DOS process is a "logical network," although it has only one station attached: the workstation function of the router or server. In addition, the router operating system treats this workstation function of the router as a "logical workstation."

A nondedicated DOS process routes data frames from the logical workstation to the operating system of the router or server. Because a nondedicated DOS process is a logical network, it must be assigned a network number that is different from the number of the network to which the network station is attached and unique on the internetwork (CCC1 in the external router and DDD1 in the server SALES). In a nondedicated file server or router, the logical workstation is assigned node number 1.

See also **Node number.**

Network backbone

A cabling system to which only file servers and routers are attached. If your network has three or more file servers, this may be an efficient way to improve network performance. The central cable handles all the network traffic, thus decreasing packet transmission time and traffic on the network.



Network backbone

Network board

A circuit board installed in each network station to allow stations to communicate with each other and with the file server.

See also **Configuration option.**

Network communication

Data transmission between network stations. Requests for services and data pass from one network station to another through a communication medium such as cabling.

Network hard disk

See **Hard disk.**

Network operator

See **User.**

Network station

Any personal computer (or other device) connected to a network by means of a network board and a communication medium. A network station can be a server, a workstation, or a router.

Network supervisor

See **User (SUPERVISOR).**

Node address

See **Node number.**

Node number

A node number identifies a network board on a network. Every station on a network must contain at least one network board. Each network board must have a unique node number to distinguish it from all other network boards in that network. In a file server with more than one network board, the node number in LAN A is designated for all traffic addressed to that server.

Node numbers can be set in a variety of ways, depending on which network board you use: (1) with jumpers or switches on boards such as Arcnet, (2) at the factory for Token-Ring and Ethernet boards, or (3) with software: the IBM *REFERENCE* diskette, for example.

See also **Network address.**

Nondedicated DOS process address

See **Network address.**

Nondedicated mode

Nondedicated file servers or routers also function as workstations. In a nondedicated file server or router, the workstation's NetWare shell runs in real mode (the first 640KB of RAM) while the file server or router software normally runs in protected mode. (Real-mode, nondedicated routers are also possible.)

The principal advantage of using a nondedicated file server or router is that an existing workstation can serve as the file server or router, eliminating the expense of buying an additional computer. The principal disadvantages are lower performance and the risk of file server or router failure if the workstation hangs.

OOO

Object

See **Bindery (Objects).**

ODI (Open Data-Link Interface)

Interconnectivity strategy that adds functionality to NetWare and network computing environments by supporting multiple protocols and drivers. ODI's benefits allow you to

- Expand your network by using multiple protocols without adding network boards to the workstation. ODI creates a "logical network board" to send different packet types over one board and wire.
- Communicate with a variety of workstations, file servers, and mainframe computers via different protocols without rebooting your workstation.
- Protect your investment because protocols send packets through any LAN driver written to ODI specifications.
- Spend less time and money on support. Because one LAN driver supports several protocols, you have fewer hardware components to support.
- Configure the LAN driver for any possible hardware configuration with NET.CFG, instead of using limited SHELL.CFG choices.
- Free up memory by using only the portions of IPX/SPX and the diagnostics that you need.

You can convert a standalone personal computer into a DOS ODI network workstation by adding one or more network boards, cabling, and the DOS ODI workstation software. If you are using a third-party network board, DOS ODI will not function unless you have a DOS ODI LAN driver for the board. Check the documentation that came with your network board for more information. As new LAN drivers and protocol transports are released, they will be available on NetWire. See "Managing DOS workstations" in *Using the Network* for instructions on using ODI drivers.

See also **Boot files.**

Operating system

See **NetWare operating system.**

Operator

See **User.**

PPP

Packet

See **Message packet.**

Packet receive buffer

See **Communication buffer.**

Parallel port

A printer interface that allows data to be transmitted a byte at a time, all eight bits moving in parallel fashion.

See also **LPT1.**

Parent directory

The directory immediately above any subdirectory. For example, SYS:ACCTS would be the parent directory of the subdirectory SYS:ACCTS\RECEIVE.

See also **Directory structure.**

Parity

See **Serial communication.**

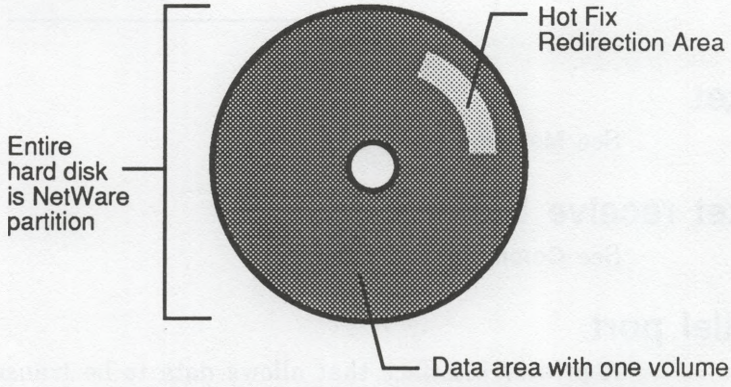
Partitions

File server hard disks can be divided into logical units called partitions. One internal hard disk can support several operating systems if each uses a different partition. For instance, you can have both an active, primary DOS partition and a NetWare partition.

Partitioning a disk is usually only helpful if a nondedicated server will boot DOS from the hard disk before loading NET$OS.EXE. (A dedicated file server boots most efficiently from a NetWare partition. It can boot from an active, primary DOS partition, but unlike a nondedicated server, the DOS partition disk space is not accessible after running NET$OS.EXE.)

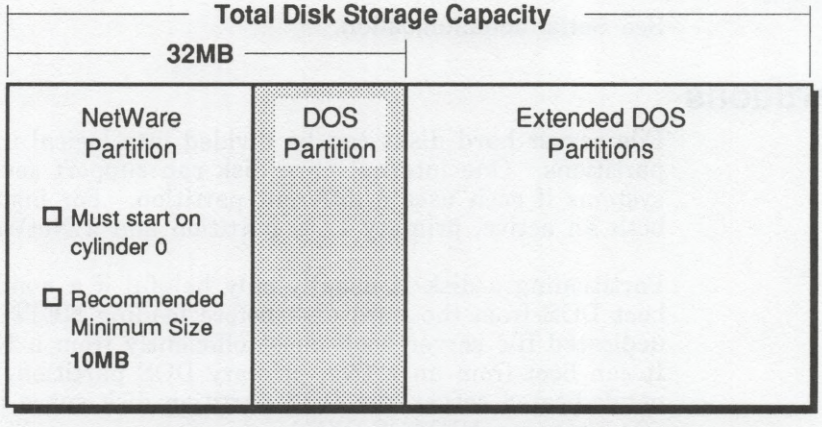
When nondedicated file server boot files are copied to the DOS partition and included in the AUTOEXEC.BAT file, the NetWare operating system will boot automatically. You need only one DOS partition; the other hard disks need only a NetWare partition.

Physically, a NetWare partition consists of a Hot Fix Redirection Area and a large data area.



To create a customized partition table with both NetWare and DOS partitions, consider the following limitations.

- The NetWare partition must start on cylinder 0.
- You can have only one NetWare partition per hard disk.
- The primary DOS partition must reside within the first 32MB of the hard disk.
- Extended DOS partitions are possible only with DOS v3.3 or above and can reside above the first 32MB.



See also **Data protection; Volume**; "File server installation" in *Installing and Maintaining the Network.*

Passive hub

A device used in certain network topologies to split a transmission signal, allowing additional workstations to be added. A passive hub cannot amplify the signal, so it must be connected directly to a workstation or an active hub.

See also **Active hub.**

Password

The word a user must type to log in to the network. NetWare allows the supervisor to specify whether passwords are required and, if so, to assign a login password to each user on the network. The supervisor can also specify whether passwords must be unique and whether they must be changed periodically. In NetWare v2.2, login passwords are encrypted at the workstation and put into a format that only the file server can decode. This format helps prevent intruders from accessing network files.

Path

A variable in command formats that represents a NetWare directory path (may include the file server, volume, directory, subdirectory, and file). Replace *path* by typing either the drive letter mapped to the directory or the complete directory path.

See also **Directory structure; Drive mappings.**

Port, hardware

A connecting component that allows a microprocessor to communicate with a compatible peripheral.

See also **Parallel port; Serial port.**

Port, software

A memory address that identifies the physical circuit used to transfer information between a microprocessor and a peripheral.

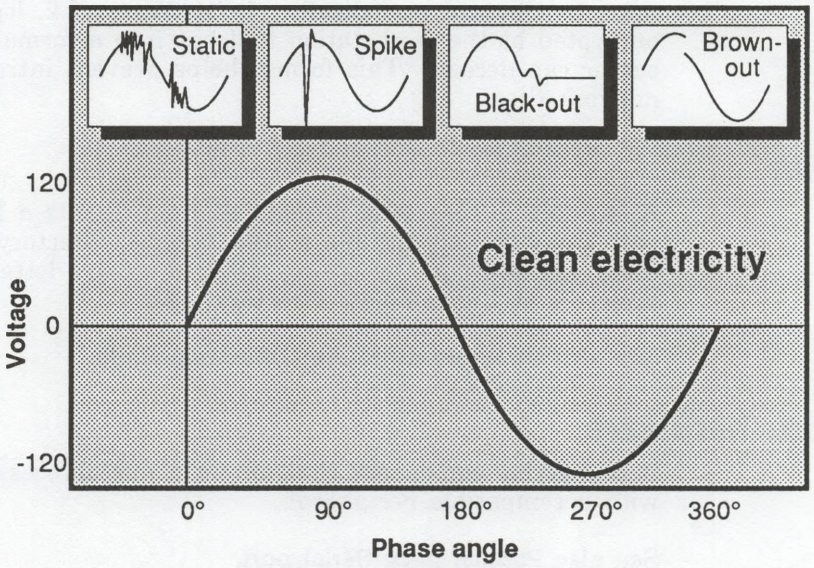
Power conditioning

Methods of protecting sensitive network hardware components against power fluctuations. All power lines connected to network components should use power conditioning equipment.

When electricity leaves a commercial power facility, it is very clean. In fact, most companies make sure the power they put out is a pure sine wave.

Unfortunately, nearly all devices create disturbances that pollute the sine wave. As power travels through a wire away from the power plant, it picks up more of these interferences. Effective power conditioning requires an understanding of how these disturbances affect the standard Alternating Current (AC) Sine Wave.

A pure AC power sine wave appears as the smooth wave in the following figure. The height of the wave is measured in volts. The wave starts at zero volts and moves to the highest point of 120 volts. The wave then cycles through a low point of -120 volts and back to zero. The speed at which it travels through this cycle is the frequency. Normal frequency is about 60 cycles per second (Hz). Anything that disrupts this wave can cause hardware or data problems and needs to be regulated.



Power disturbances can be categorized in several ways. A transient, sometimes called a spike or surge, is a very short, but extreme, burst of voltage. Noise or static is a smaller change in voltage. Brownouts and blackouts are the temporary drop in or loss of electrical power. Three types of protection against these three events are available: suppression, isolation, and regulation. The supervisor should verify that the appropriate combination of these three types of protection is properly installed.

Suppression protects against transients. The most common suppression devices are surge protectors that usually include circuitry to prevent excess voltage. Although manufacturers originally designed surge protectors to prevent large voltage changes, most have also added circuitry to reduce noise on the line.

Isolation protects against noise. Ferro-resonant isolation transformers use a transformer within the circuitry to envelop the sine wave at a slightly higher and lower voltage. Any voltage irregularity that extends beyond this envelope is clamped. Isolation transformers are usually very expensive.

Regulation protects against brownouts and blackouts. Regulation modifies the power wave to conform to a nearly pure wave form. The Uninterruptible Power Supply (UPS) is the most commonly used form of regulation. A UPS comes in two varieties, on-line and off-line.

An on-line UPS actively modifies the power as it moves through the unit. This is closer to true regulation than the off-line variety. If a power outage occurs, the unit is already active and continues to provide power. The on-line UPS is usually more expensive but provides a nearly constant source of energy during power outages.

The off-line UPS monitors the AC line. When power drops, the UPS is activated. The drawback to this method is the slight lag before the off-line UPS becomes active. Most commercial UPS systems are fast enough to offset this lag.

Because UPS systems are expensive, most companies attach them only to the most critical devices, such as file servers, routers, and hard disk subsystems. Attaching a UPS to a file server enables the server to properly close files and rewrite the system directory to disk. Unfortunately, most programs run on the workstation and data stored in RAM is not saved during a power outage unless each workstation has its own UPS. If the UPS doesn't have its own form of surge protection, it is a good idea to install a surge protector to protect the UPS from transients.

Proper use of power conditioning devices greatly reduces network maintenance costs. Make sure that the proper amperage is available for each system and that all outlets are grounded. Dedicated power lines should provide ample amperage. Power conditioning devices connected to poorly grounded outlets offer very little protection.

Studies have shown that total network maintenance costs are higher with line-surge suppressors and ferro-resonant isolation transformers alone, than with uninterruptible power supplies.

See also **UPS monitoring.**

Print device

See **Printing.**

Print function

A printer command (or escape sequence) that determines the characteristics of a print job. For example, a print function can specify the font.

Print job configuration

A group of characteristics that determine how a job is printed. The characteristics may include the mode, the form, the number of copies, and the particular printer to be used. Users can create print job configurations using the PRINTCON utility.

See also **Print mode.**

Print mode

A sequence of print functions (also called printer commands and escape sequences) that determines the appearance of the printed file. A print mode can define the style, size, boldness, and orientation of the typeface. The SUPERVISOR uses PRINTDEF to create and designate print modes, allowing users to quickly select a combination of print functions.

Print queue

See **Printing.**

Print queue operator

See **Printing.**

Print server

See the *NetWare Print Server* manual.

Print server operator

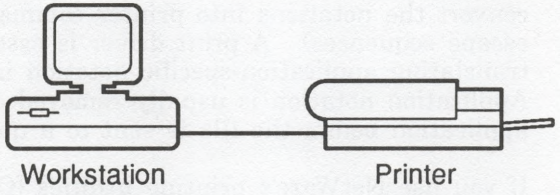
See the *NetWare Print Server* manual.

Printing

This section provides an overview of the printing services available within the NetWare v2.2 operating system. It does not describe the NetWare print server (PSERVER.EXE and PSERVER.VAP), a process that is independent of the NetWare operating system. If you intend to use the NetWare print server, see the *NetWare Print Server* manual.

Printing on a network. To network users, printing from a network workstation seems the same as printing from a standalone workstation, but there are differences.

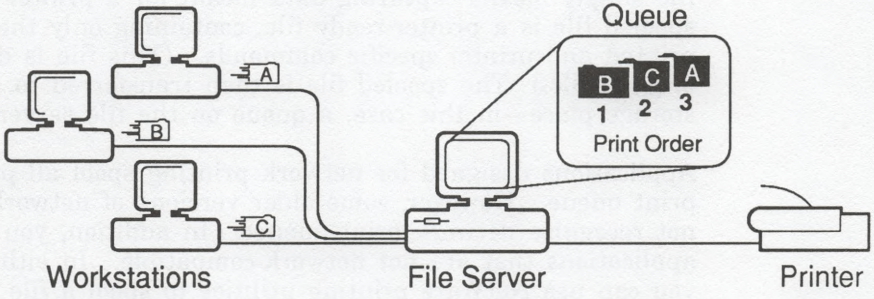
When a user at a standalone workstation sends a print job to a locally attached printer, the job travels from the workstation's printer port directly to the printer for processing.



Standalone printing environment

However, when a user on a network workstation sends a print job to a network printer, the job travels from

- The network workstation
- To a print queue on the file server
- To a printer assigned to the print queue



Network printing environment

When a print job leaves a network station, it is stored temporarily in a print queue (a subdirectory on the file server) until the assigned printer is ready to print the job.

Starting at the workstation. A print job begins at the workstation as a block of data. Many applications attach headers, footers, and even internal characters to the data block that contain information useful only to the application.

To transform this data into a print job, these notations must be removed or converted into printer-specific commands. The notations of a word processing application surrounding characters on the screen, such as "Bold" or "10pt," can't be read by the printer. They must be converted into printer commands by the application to designate how a paragraph, a word, or even a character will be printed.

The application must use a print driver for your specific printer to convert the notations into printer commands (such as PostScript or escape sequences). A print driver is essentially a conversion table for translating application-specific notation into printer commands. Application notation is usually removed or converted within the application before the file is sent to a queue.

If you use NetWare's printing utilities (CAPTURE, NPRINT, and PCONSOLE) to print a file, they will attach a header to your files containing printer-specific commands that tell the printer how to print the entire file. These printer commands include the number of copies, banner page information, and, if you use PRINTCON to create a print job configuration or set a default in PCONSOLE, any printer commands you choose for your printer. For instance, if you want to reset your printer after printing, you can select a reset command and NetWare will attach it to the end of your file.

Spooling to the queue. Once the application notation has been removed or converted, the file must be *spooled* to the print queue. Spooling a file simply means capturing data meant for a printer into a file. A spooled file is a printer-ready file, containing only the data to be printed and printer-specific commands. (This file is different from the original file.) The spooled file is then transferred to a temporary storage place—in this case, a queue on the file server.

Applications designed for network printing spool all print jobs to a print queue. However, some older versions of network applications do not recognize network print queues. In addition, you may use some applications that are not network-compatible. In either of these cases, you can use NetWare printing utilities to spool a file to a print queue.

If you use an older version of a network application that spools print jobs to network *printers* rather than to print queues, you need to use SPOOL at the file server to redirect the job. SPOOL links the printer number specified by the application to the print queue you select.

If you need to print from an application not designed for a network, you can use the CAPTURE utility to spool the file. CAPTURE reroutes the print job from your workstation's parallel port to a print queue on the file server.

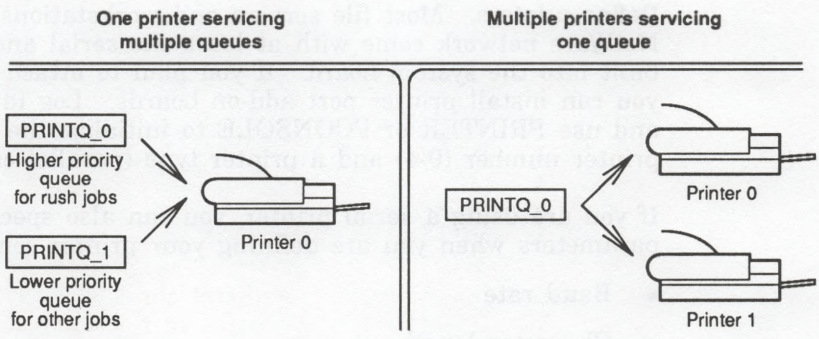
Queues and queue management. Both NetWare printing utilities and applications designed for network printing send print jobs to queues. Queues are subdirectories in the SYS:SYSTEM directory that store print jobs. Each queue can be assigned to one or more printers attached to the file server. The order in which print jobs go to the printer depends on NetWare's queue management system.

The queue management system arranges print jobs in a queue according to the time they arrive, which usually means they are printed on a first in/first out basis. However, queue users can set print file holds and timed releases on a job, and a queue operator can change the sequence of the jobs waiting in the queue. Queue management tracks the status of jobs, releasing them to the assigned printer at the proper time, and in the proper order.

Assigning queues to printers. When you define a printer, you specify which queues the printer will service. Assigning one queue to each printer simplifies your printing setup, but you may have more complicated needs.

One printer can service several queues. For example, you could set up a high-priority queue that is serviced before any other queue. You can specify priority (from 1 to 10) when you assign the queue to the printer.

In addition, multiple printers can service a single queue. For example, you could have two identical printers printing jobs from one queue, enabling you to maintain a first-come, first-served approach to printing large numbers of print jobs.



Assigning queues to printers

Setting up the network print path. You set up the path for network printing after you have generated the NetWare v2.2 operating system. Unlike previous versions of NetWare v2.*x*, the operating system does not create default print queues and spooler assignments automatically. Rather, you create print queues, define printers, and assign the queues to printers at the file server console.

Create print queues. When you create a print queue, a corresponding directory is created in the SYS:SYSTEM directory. Each print job is stored as a file in the directory created for that queue. You can create print queues with either QUEUE at the file server or PCONSOLE at a workstation.

- **Queue operators.** When you create a print queue, user SUPERVISOR is automatically assigned as a print queue operator.

  Using PCONSOLE, the supervisor can designate other users as queue operators as necessary. Queue operators can edit any user's print job in the queue, delete any job from the queue (even if it is being printed), and modify the queue status by changing the operator flags. Queue operators can also change the order in which print jobs will be serviced.

- **Queue users.** To send print jobs to a queue, a network user must be designated a print queue user. Members of the group EVERYONE automatically become print queue users when the print queue is created. As a result, all network users (as members of the group EVERYONE) can send print jobs to the print queue. If these assignments are not satisfactory, you can change them using PCONSOLE.

Define printers. Most file servers and workstations approved for a NetWare network come with at least one serial and one parallel port built into the system board. If you plan to attach additional printers, you can install printer port add-on boards. Log in as SUPERVISOR and use PRINTER or PCONSOLE to initialize the port by specifying a printer number (0-4) and a printer type (parallel or serial).

If you are using a serial printer, you can also specify the following parameters when you are defining your printer configuration:

- Baud rate
- Character length
- Stop bits
- Parity
- XON/XOFF protocol

For a discussion of these parameters, see **Serial communication.**

Assign queues to printers. When all printers are defined and queues are created, you must assign the queues to printers with PRINTER. When you assign a queue to a printer, you enable a file server process that transfers the print job from the queue to the printer.

Printing files. When you have set up the network print path, you can print from any application designed for network printing, or you can print with the NetWare printing utilities.

Printing from applications designed for network printing. Many applications are designed for network printing. The application documentation includes specific directions for printing files.

If you use applications written for earlier versions of NetWare, they may send print jobs to printer numbers rather than to print queues. If so, you must set up spooler assignments at the file server console.

Spooler assignments translate the printer number used by the application into a queue that NetWare can recognize. When an application tries to send a job to a printer, the spooler intercepts that job and puts it into a queue. The job is then serviced by the printer assigned to that queue.

You should save the printer definitions and spooler and queue assignments by including them in the system AUTOEXEC file (using "Supervisor Options" in SYSCON). Each time the file server comes up, the spooler assignments are set up automatically.

Printing from applications not designed for network printing. If you are using applications that are not designed for network printing, NetWare provides four utilities to help you print files: CAPTURE, ENDCAP, NPRINT, and PCONSOLE.

You should specify a default print queue for CAPTURE and NPRINT by setting up a spooler assignment with the SPOOL command at the file server. If you do not specify a queue, the print job is sent to the queue Spooler 0 has been mapped to. If it has not been mapped to a queue, you will receive an error message and your job will not print.

CAPTURE/ENDCAP. Use CAPTURE to print screen displays, to save data to a network file, and to print from applications not designed for network printing.

CAPTURE is a command line utility that captures print data sent to a workstation's parallel port and spools it to a network file or a network print queue. You can specify printing parameters at the command line or set up a print job configuration as a shortcut. You can also include CAPTURE in your system or individual login script. ENDCAP ends the CAPTURE and directs print commands back to the workstation's parallel port.

Printer numbers are no longer supported with CAPTURE. If you are upgrading from NetWare v2.*x* and have included the printer option (CAPTURE p=*x*) in your login script, you now need to use the queue option (CAPTURE q=*x*).

NPRINT. Use NPRINT to print files created in applications or as ASCII text files.

NPRINT is a command line utility that sends files stored on a disk (local or network) to a specified print queue. Files must be printer-ready. You can specify printing parameters at the command line or set up a print job configuration as a shortcut.

To print a file with NPRINT, you must specify the directory path and filename of the specific file you want sent to the queue. You can use wildcard characters to print more than one file at a time. NPRINT sends your files to the print queue immediately.

PCONSOLE. Use PCONSOLE to print files created in applications or as ASCII text files. Like NPRINT, PCONSOLE routes the files to a specified print queue. However, PCONSOLE is a menu utility, so you select your file and specify printing parameters from a menu.

PCONSOLE also allows you to create queues, assign operators and users, and monitor all queued print jobs. If you are a supervisor, you can delete, hold, or change the service sequence of any queued print jobs.

Customizing the printing environment. If you will be printing frequently from applications that are not designed for network printing, you can customize your printing environment with PRINTDEF and PRINTCON. These utilities create print job configurations to control the network print process for you.

Print job configurations simplify printing with CAPTURE, NPRINT, and PCONSOLE. When you use a print job configuration with these utilities, you do not need to manually enter printing instructions each time you print a file.

We suggest you use PRINTDEF and PRINTCON in two cases only:

- To reset your printer to default fonts after using different printing setups.

  For example, if you are printing spreadsheets and letters on the same printer, you may have some problems with the printer resetting after each print job.

- To specify different forms or print configurations when you are using CAPTURE, NPRINT, and PCONSOLE.

PRINTDEF. Use PRINTDEF to select a print device (such as a printer or plotter) and to select printer commands for that device. You can assign any number of printer commands to a mode and then use PRINTCON to attach the mode to your print job.

NetWare includes print device definitions for commonly used printers. These definitions are automatically placed in the SYS:PUBLIC directory during installation. Each definition contains a list of printer commands that your print device can understand. However, you must copy the definitions that you need to a PRINTDEF database before you can select printer commands from them.

If the print device you use is not on the existing list, you can import additional print device definitions from other file servers or storage media. You can also manually create print device definitions that include the printer commands particular to your print device.

PRINTDEF also allows you to define different forms for odd-sized paper such as envelopes, labels, and chart paper.

PRINTCON. Use PRINTCON to create print job configurations, which can include the modes and forms you created in PRINTDEF as well as other instructions for the network print process. You can use the print job configurations when you print with NetWare utilities.

Some of the useful parameters you can include in a print job configuration include

- Banner page information
- Number of copies
- File server, queue, and printer
- Timeout count
- Auto endcap

All print job configurations for users are stored in each user's mail directory in a file named PRINTCON.DAT. You can copy new configurations into these mail directories. However, since all configurations are stored in PRINTCON.DAT, doing so overwrites all previously-defined configurations in the user's old PRINTCON.DAT.

The first print job configuration you create becomes the default. When you create other configurations, you can select a different default, usually the one you use most often. The default configuration is used by NPRINT and CAPTURE unless you specify another configuration at the command line.

If you don't use the default printer, choose a configuration with a mode that contains commands appropriate for the new printer.

Prompt

A character or message (generated by the software) that appears on the display screen and requires a response (such as a command or a utility name) from the user.

Standard types of prompts include the following:

- The DOS prompt, which displays one of the local drives (A to E) followed by a caret: A>
- The network prompt, which displays one of the network drives (F to Z) followed by a caret: F>
- The file server console prompt, which displays a colon (:)
- The OS/2 prompt, which displays a drive letter in brackets: [B]

Property

See **Bindery.**

Protected mode

Mode of operation with 80286 and later processors that uses RAM beyond 1MB (megabyte).

The 80286 processor can run in either of two modes: real or protected. In real mode, it emulates an 80286 (it accesses a maximum of 640KB of RAM and runs only one software application at a time).

Protected mode allows the 80286 processor to access up to 16MB of memory. It uses a 24-bit address bus. Since a bit can have one of two values, raising the base number of 2 to the power of 24 is equal to 16,777,316 unique memory addresses. Each memory address can store one byte of information (16,777,216 bytes equals 16MB).

Protected mode operation also makes it possible to run more than one application at once and to handle more processes because more memory is available. Processes can be requests from an operating system or an application to perform disk I/O, memory management, printing, or other functions.

Processes are assigned priority numbers in protected mode. The processor gives priority to those with higher numbers. Operating system processes always have higher priority than application processes. If protected mode is used, the operating system can make the most efficient use of all computer resources.

See also **Real mode.**

Protocol

See **NCP services.**

Protocol, NetWare Core

See **NCP services.**

Public access

A security condition that gives all NetWare users access rights to a particular directory. For example, all NetWare users must be able to access NetWare utilities. For this reason, NetWare utilities are usually placed in a directory (SYS:PUBLIC) where all users have Read and File scan rights for files in that directory.

PUBLIC directory

The SYS:PUBLIC directory is created automatically on the SYS volume during network installation and cannot be deleted. The NetWare utilities, as well as the .OVL and .DAT files necessary to run the menu utilities, are copied into the PUBLIC directory during installation. All NetWare users need a search drive mapped to the PUBLIC directory. This is usually done in the system login script. The group EVERYONE is assigned Read and File Scan rights to this directory when it is created.

Public files

Files that need to be accessed by all NetWare users. By convention, they are located in the SYS:PUBLIC directory. This general access directory is created automatically during network installation and cannot be deleted. NetWare utilities, help files, and some message and data files (such as the system login script file, NET$LOG.DAT) are public files that all NetWare users have Read and File scan rights to.

QQQ

Queue

See **Printing.**

RRR

RAM buffer address

See **Base memory address.**

Read Audit attribute

See **Security (Attribute security).**

Read Only attribute

See **Security (Attribute security).**

Read right

See **Security (Rights security).**

Read Write attribute

See **Security (Attribute security).**

Read-after-write verification

See **Data protection.**

Real mode

Mode of operation with 8086 and later processors that uses a maximum of 1MB (megabyte) of addressable RAM and can run only one software application at a time. Real mode allows 80286, 80386, or 80486 processors to emulate an 8086 processor but perform better than the 8086 because they operate at a faster clock rate. A router with an advanced processor but no extra memory should run in real mode. Real mode is limited to a maximum of 1MB of addressable memory because the 8086 processor uses a memory address bus of 20 bits.

Since a bit can have one of two values, raising the base number of 2 to the power of 20 is equal to 1,048,576 unique memory addresses. Each memory address can store 1 byte of information (1,048,576 bytes equal 1MB).

See also **Protected mode.**

Record locking

A feature of the NetWare operating system that prevents several users from gaining simultaneous access to the same record in a shared file, thus preventing overlapping disk writes and ensuring data integrity.

Recursive copying

Copying, not only a specified source directory, but also all subdirectories and files, to a destination directory.

Recursive copying copies all directories and files of a logical drive to the destination. Directory trustee rights and directory and file attributes are not copied. The Maximum Rights Masks of the copied directories contain all rights. The DOS XCOPY and BACKUP utilities and NetWare FILER and NCOPY utilities use recursive copying.

Redirection Area

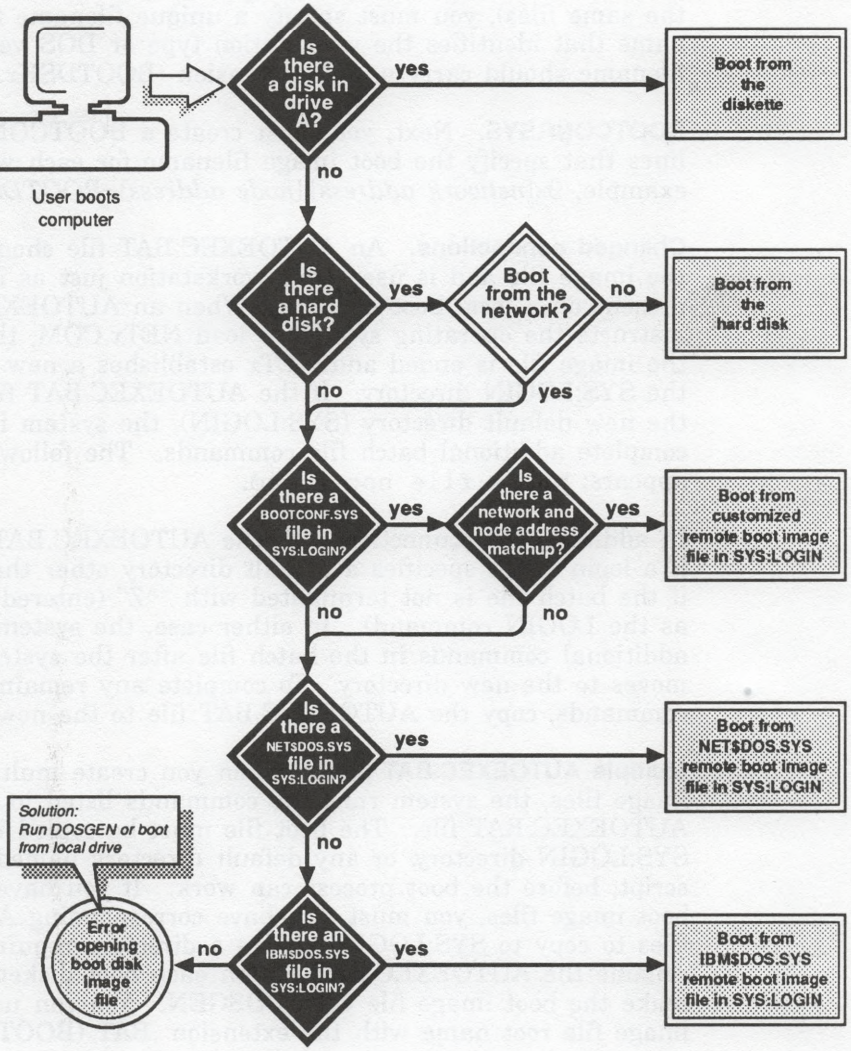
A small portion of the hard disk that is set up as a table to hold data blocks that are "redirected" from bad block locations on the disk. The Redirection Area is set up during installation.

See also **Data protection.**

Remote boot

Remote boot allows a user to boot a workstation from remote boot image files on a file server rather than from boot files in the workstation's local drive. Before you can use remote boot, you must install a remote reset ROM chip on the workstation's network board and run DOSGEN to upload a workstation's boot files into an image file on the file server. The default name of this remote boot image file is NET$DOS.SYS (IBM$DOS.SYS in v2.0a). See "Managing DOS workstations" in *Using the Network.*

The following figure illustrates how the remote boot ROM directs the boot process and all read requests to the remote boot image file on the file server. The ROM shuts down and allows ROM-BIOS to take over if you boot from a local diskette or hard disk.



The remote boot process still considers SYS:LOGIN as drive A, so the workstation drive A light may turn on while the workstation boots from the network.

The default server is the first server that responds to the workstation. On a large network or internetwork, the first server to respond could vary, so the remote boot image files must be copied to the LOGIN directories of each file server that could possibly respond.

If several boot image files are required (if workstations don't boot with the same files), you must specify a unique filename for each. Choose a name that identifies the workstation type or DOS version. The new filename should carry a .SYS extension (BOOTDSK*x*.SYS, for example).

BOOTCONF.SYS. Next, you must create a BOOTCONF.SYS file with lines that specify the boot image filename for each workstation. For example, 0x[*network address*],[*node address*]=*BOOTDSKx.SYS*.

Changed connections. An AUTOEXEC.BAT file should be included in the image file and is used by a workstation just as if the file were present on a local boot diskette. When an AUTOEXEC.BAT file instructs the operating system to load NET*x*.COM, the connection to the image file is ended and NET*x* establishes a new connection with the SYS:LOGIN directory. If the AUTOEXEC.BAT file is not found in the new default directory (SYS:LOGIN), the system is unable to complete additional batch file commands. The following message appears: `batch file not found`.

In addition, the connection with the AUTOEXEC.BAT file could be lost if a login script specifies a default directory other than SYS:LOGIN, or if the batch file is not terminated with "^Z" (entered on the same line as the LOGIN command). In either case, the system looks for additional commands in the batch file after the system connection moves to the new directory. To complete any remaining batch file commands, copy the AUTOEXEC.BAT file to the new default directory.

Multiple AUTOEXEC.BAT files. When you create multiple remote boot image files, the system runs the commands listed in the image file's AUTOEXEC.BAT file. The boot file must be copied into the SYS:LOGIN directory, or any default directory named in the login script, before the boot process can work. If you have several remote boot image files, you must also have corresponding AUTOEXEC.BAT files to copy to SYS:LOGIN. Since a directory requires unique names, rename the AUTOEXEC.BAT file on each boot diskette before you make the boot image file with DOSGEN. You can use the same boot image file root name with the extension .BAT (BOOTDSK*x*.BAT).

When the operating system first uses the image file, it looks for executable commands in a file specifically named AUTOEXEC.BAT. You must, therefore, create an AUTOEXEC.BAT file for each boot diskette containing one command: BOOTDSK*x*.BAT. When the workstation boots from the boot image file, this AUTOEXEC.BAT file directs the system to use the BOOTDSK*x*.BAT file for all subsequent batch file commands. You must copy the BOOTDSK*x*.BAT files to SYS:LOGIN and subsequent directories just as the single AUTOEXEC.BAT file is copied for a single remote boot image file.

See **Boot files;** "Managing DOS workstations" in *Using the Network*.

Remote connection

A connection between a LAN and a workstation or network, often using telephone lines. A remote connection allows data to be sent and received across greater distances than those allowed by normal cabling.

Remote reset

See **Remote boot.**

Remote workstation

A terminal or personal computer connected to the LAN by a modem. A remote workstation can be either a standalone computer or a workstation on another network.

Removable media

See **Disk.**

Removable volume

See **Disk.**

Resource

In NetWare installation programs, any device, feature, circuit board, or built-in circuitry that uses one or more of the following to communicate with the file server's microprocessor: interrupt lines, DMA lines, I/O addresses, or memory addresses (RAM or ROM).

Rights

See **Security.**

Root directory

The highest directory level in a hierarchical directory structure. With NetWare, the root directory is the volume; all other directories are subdirectories of the volume.

See also **Directory structure.**

Router

A router manages the exchange of information (in the form of data packets) between network cabling systems.

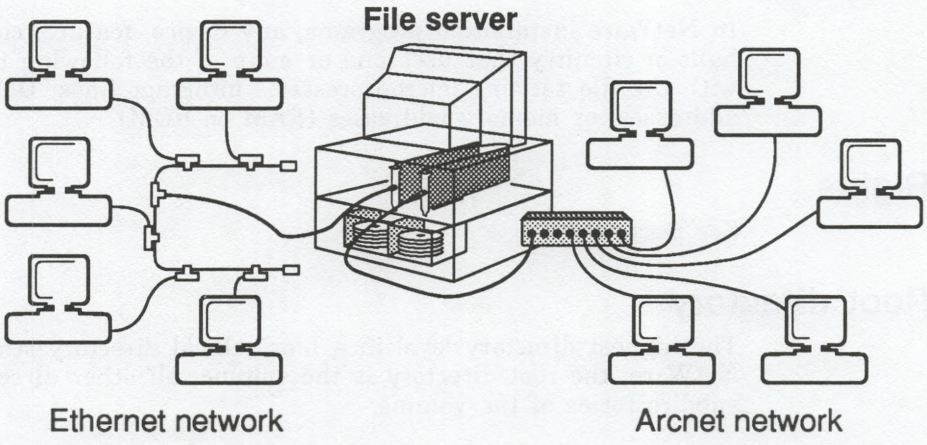
NetWare router vs. traditional bridge. A NetWare router, unlike a traditional bridge, does more than just transfer data packets between networks that use the same communications protocol.

A NetWare router is "intelligent." It not only passes packets of data between different cabling systems, but also routes the packets through the most efficient path.

A NetWare router can also connect cabling systems that use different kinds of transmission media and different addressing systems. For example, a NetWare router can connect a network using the Ethernet addressing structure and RG/58 coaxial cable to another network using the Arcnet addressing structure and RG/62 coaxial cable.

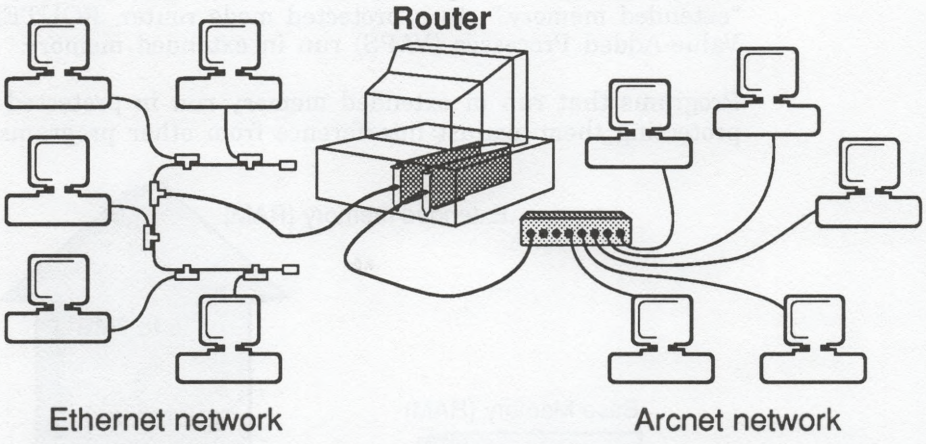
Internal vs. external. These are the two major types of NetWare routers.

An **internal router** runs as part of a file server. It connects separate network cabling topologies or separate networks by way of the file server's NetWare operating system.



Internal router

An **external router** runs in a networked computer that is not a file server and manages packet routing with ROUTER.EXE.



External router

Local vs. remote. When a router is used within the cable length limitations for its LAN drivers, it is a local router. If the router is connected beyond its driver limitations or through a modem, it is a remote router.

You can find the cable length limits for your LAN drivers in the NetWare installation supplements.

Dedicated vs. nondedicated. The decision to use a dedicated or a nondedicated router involves considering the tradeoff between hardware cost and the risk of router failure.

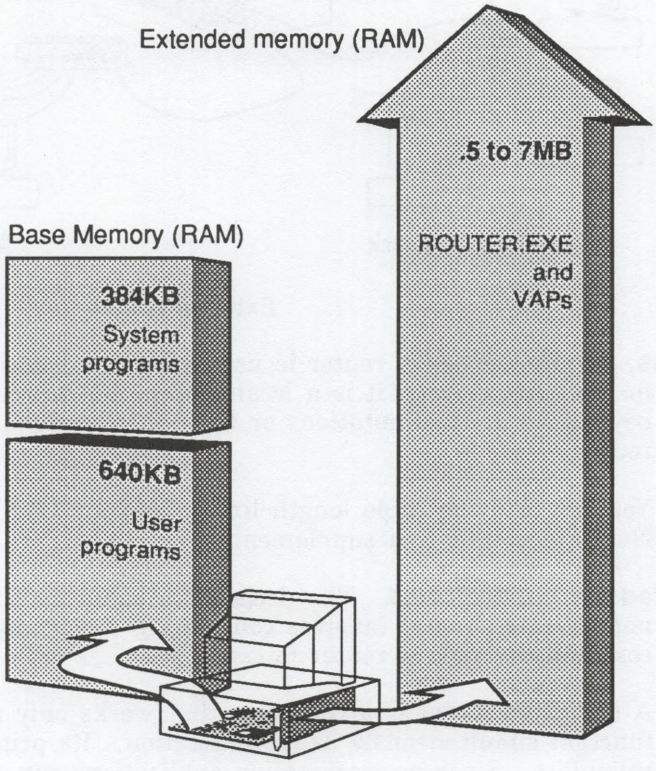
A **dedicated router** is a computer that works only as a router; it cannot function simultaneously as a workstation. Its principal advantage is reliability. Since no workstation applications run on this kind of router, applications cannot hang and cause the router to stop operating. Router failure not only stops data sharing between networks, but it can bring down any workstation sessions connected to the file server via the router.

A **nondedicated router**, on the other hand, can function simultaneously as a router and as a workstation. Its principal advantage is that an existing workstation can serve as the router, eliminating the expense of buying an additional computer. In addition to the risk of applications hanging, you will have lower performance with nondedicated routers.

Protected mode vs. real mode. The type of microprocessor your router has and the amount of memory installed determine whether your router (ROUTER.EXE) should run in protected or real mode.

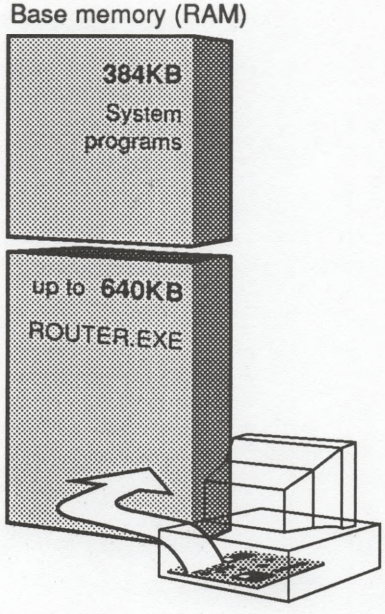
A **protected mode router** contains an 80286, 80386, or 80486 microprocessor and can have up to 8MB of RAM (8MB is a NetWare router limitation). Anything above 1MB of base memory is called "extended memory." In a protected mode router, ROUTER.EXE and Value-Added Processes (VAPS) run in extended memory.

Programs that run in extended memory run in protected mode, protecting them against interference from other programs.



Protected mode router

A **real mode router** contains an 8086 or 8088 microprocessor and can access only 1MB of memory. Machines with 80286, 80386, or 80486 microprocessors set to run in real mode act like an 8086.



Real mode router

Routing table. Each file server and router on a NetWare v2.2 internetwork contains an internetwork router. Each router constantly broadcasts its own current status and updates the distances to and the locations of other routers in its routing tables; the router also chooses the most efficient route whenever a change of routing occurs in the internetwork (the file server goes down or a new network is added).

For installation instructions, see "Router installation" in *Installing and Maintaining the Network.*

ROUTER.CFG

See **Boot files.**

Routing buffer

See **Communication buffer.**

RPL (Remote Program Load)

IBM's term for remote boot or remote reset—see **Remote boot.**

SSS

Salvageable files

Files deleted in the last ERASE or DELETE command that can be restored with SALVAGE. Files deleted in earlier commands are lost permanently.

Related utilities: SALVAGE (see *Using the Network*).

SCSI (Small Computer System Interface)

An industry standard that sets guidelines for connecting peripheral devices and their controllers to a microprocessor. The SCSI defines both hardware and software standards for communication between a host computer and a peripheral. Computers and peripheral devices that are designed to meet SCSI specifications are assured a large degree of compatibility.

SCSI bus

Iinterface that connects additional HBAs to controllers and hard disks. Make sure connected peripherals are properly terminated and addressed.

See also **Hard disk.**

Search drive

A drive that is automatically searched by the operating system when a requested file is not found in the current (default) directory. A search drive allows a user working in one directory to transparently access an application or data file that is located in another directory.

See also **Drive mappings.**

Security

NetWare provides an extensive three-level security system to control access to information stored on network volumes:

- Login security
- Rights security
- Attribute security

NetWare security determines

- Who can access the network
- What resources (directories and files) users can access
- What users can do with those resources (for example, read or modify a file)

This entry explains NetWare security, provides guidelines for planning security, and lists utilities for establishing and monitoring security.

Login security. Login security determines which users can access the file server, when they can work, and what workstations they can work from. The network supervisor establishes login security by assigning usernames, requiring passwords, and setting up account restrictions.

Only network supervisors and Workgroup Managers can create user accounts. To access the file server, users must know a username (and its corresponding password, if one is required). The usernames are kept in the file server's bindery and are assigned properties. As you assign properties to usernames, you grant the users sufficient security clearance to do their jobs. All users are automatically assigned properties for a password and membership to the group EVERYONE.

If a username is spelled incorrectly or if the username does not exist on the server, access will be denied; if the user has a password, access will not be granted until the correct password is entered. The generic "Access Denied" message prevents unauthorized users from knowing whether the username, the password, or both failed.

Passwords are optional. However, if you don't require passwords, any person who knows a valid username can access the file server. A password's confidentiality is protected by NetWare. When you type a password at a workstation, the password is not displayed on the monitor. NetWare encrypts the password at the workstation and stores it on the file server in its encrypted form.

If you require passwords, you can either assign and change user passwords yourself or assign an initial password and allow users to choose and change their own passwords. If you allow users to change their own passwords, you can increase password security by requiring any or all of the following:

- A minimum password length (default 5 characters, maximum 20) to prevent users from using short, easy-to-guess passwords.
- A periodic change in the password (default every 40 days) to prevent users from keeping a password indefinitely.

- A unique password to prevent users from alternating between favorite passwords. The file server remembers the last eight passwords and requires that passwords be used for at least one day (so a user cannot change eight passwords in one day).
- A limited number of grace logins after password expiration (default 6) to prevent unlimited use of an expired password.

Account restrictions (station, time) protect the network from intruders by controlling when and where a user can log in.

- Station restrictions specify which workstations a user can use and how many workstations a user can log in to simultaneously.
- Time restrictions restrict users to specific days and hours.
- Account restrictions lock a user's account when certain limits are exceeded. When an account is locked, no one can log in to the file server using that username. Accounts can be locked automatically when an account expires, when an account's balance is depleted, and when a set number of incorrect password attempts is exceeded (intruder detection). Account expiration or a depleted balance both lock an account permanently. Too many attempts to log in with an incorrect password lock the account temporarily (the SUPERVISOR specifies how long the account is locked).

See also "Managing accounting," "Logging in and out," and "Managing users and groups" in *Using the Network*.

Related utility: SYSCON (see *Using the Network*).

Rights security. Rights security controls what a user is allowed to do with files in specific directories and subdirectories.

Understanding rights. NetWare uses seven rights (each represented by its initial) to control file access in a directory.

NetWare v2.2	Earlier versions of NetWare
R Read	**R**ead and **O**pen
W Write	**W**rite and **O**pen
C Create	**C**reate
E Erase	**D**elete
M Modify	**M**odify
F File scan	**S**earch
A Access control	**P**arental

NetWare utilities display the initial letters of these rights between brackets, as shown below.

[R W C E M F A]

By convention, if some rights have been revoked or are not assigned, the absence of each is indicated by a blank space as shown below.

[R F]

Rights can be assigned to users (trustee rights) or to directories (via a Maximum Rights Mask). They control general access to directory files as follows:

Right	Description
Read	Allows users to open and read files.
Write	Allows users to open and write to existing files.
Create	Allows users to create directories and files.
Erase	Allows users to delete a directory, its files, and subdirectories.
Modify	Allows users to change directory and file names and attributes (with File scan), but not their contents.
File scan	Allows users to see files.
Access control	Allows users to change trustee assignments and the Maximum Rights Masks.

The combination of Trustee rights and the directory's Maximum Rights Mask determine which of the above seven rights is effective in a directory.

- **Trustee** rights (File scan, for example) allow specific users or groups particular rights to files in a directory and apply to all subdirectories until redefined (in other words, trustee rights flow down through the directory structure). The network supervisor assigns rights or security equivalence to users or groups, which they can exercise if the directory's Maximum Rights Mask includes the same rights.
- **A Maximum Rights Mask** that includes all seven rights is automatically allocated to each directory when it is created. If you want to limit access to a directory without changing trustee rights, delete rights from that directory's Maximum Rights Mask. Changes to the Maximum Rights Mask of a given directory affect the user's effective rights in only that directory (in other words, the Maximum Rights Mask does not flow down through the directory structure).

- **Effective rights** are the rights a user can actually exercise in a given directory and include assigned trustee rights not filtered out by the current directory's Maximum Rights Mask.

The following figure illustrates how trustee rights and a directory's Maximum Rights Mask combine to determine effective rights:

Trustee assignments	R	W	C			F	
Maximum rights mask	R		C	E	M	F	A
Effective rights	R		C			F	

If, however, a user creates a subdirectory under the directory referred to in the above chart, the Maximum Rights Mask for the newly created subdirectory would again contain all rights.

A user's effective rights in a directory or file are also conditioned by directory and file attributes (see **Attribute security** on page 139). Attributes take precedence over a user's effective rights. For example, if a file is flagged with the Read-Only attribute, users will not be able to write to the file, rename it, delete it, or create another file of the same name, regardless of their effective rights. Even user SUPERVISOR can't change the file without first changing the file's attribute to Read-Write.

To view effective rights, see FILER; RIGHTS; TLIST; WHOAMI /R (in *Using the Network*).

Assigning rights. You can grant any combination of rights, although some combinations are not useful:

- You could grant a user only Read and File scan rights, but if the application this user runs creates temporary files when accessed, this user will not be able to work because the Cr%%eate, Erase, and Modify rights have not been granted.
- You could create a new directory and delete the Access Control right from the Maximum Rights Mask, but no one, except the supervisor, would be able to assign directory rights to any subdirectories in that directory.

Grant rights carefully—particularly the Access control right. Users with too many rights can delete, corrupt, or steal data. Users with too few rights will not be able to do the work assigned to them.

Some common tasks and the rights required to do them follow.

Task	Rights required
Read from a closed file	Read
See a filename	File scan
Search for files in a directory	File scan
Write to an existing file	Write, Create, Erase
Create and write to a file	Create, Write
Copy or NCOPY files into a directory	Create, Write
Remove an empty subdirectory	Erase
Delete a file	Erase
Change subdirectory attributes	Modify
Change file attributes	Modify, File scan
Rename a subdirectory	Modify
Rename a file	Modify, File scan
Change the Maximum Rights Mask	Access control
Change trustee assignments	Access control

When assigning rights to application directories, check the application's documentation. If possible, separate the files that users create when they use the application from the executable files needed to run the application. Normally users only need R and F rights to directories containing executable files, while they need R, F, C, E, and M rights to directories in which they create and modify files. If the applications (and thus the executable files) are mapped to a search drive, users can access the applications from another directory where they have the additional rights needed to create and modify files.

To grant, modify, or view trustee rights, see FILER, GRANT, REMOVE, REVOKE, SYSCON, and "Managing users and groups" in *Using the Network*.

To modify a directory's Maximum Rights Mask, see FILER and "Organizing and accessing files" in *Using the Network*.

Attribute security. Attribute security assigns special properties to individual directories or files. Attribute security overrides rights granted with trustee rights and can prevent tasks that effective rights would allow. For example, attributes can be used to prevent the following:

- Copying a file
- Deleting a file
- Viewing a file or a directory

Attributes are also used for the following:

- Controlling whether files can be shared (whether only one user or many users can access files at the same time)
- Marking files as modified so that backup utilities can select only the files that have been modified
- Protecting files from data corruption by ensuring that either all changes are made or no changes are made when a file is being modified

If users have the Modify right in the directory, they can change the attributes of files and subdirectories and complete any task allowed with their effective rights.

The chart on the next page summarizes directory and file attributes and their functions.

Attributes	Letter	Directory	File	Description
Archive needed	**A**		✓	Identifies files modified after last backup. Assigned automatically. DOS's Archive bit.
Execute Only	**X**		✓	Prevents copying or backing up files. Assign only to files with an .EXE or .COM extension (program files). Only a supervisor-equivalent user can assign this file attribute. The attribute cannot be removed, so it should only be assigned if a backup copy of the file exists. CAUTION: Some programs will not execute properly if flagged Execute Only.
Hidden	**H**	✓	✓	Hides directories and files from DOS DIR scans and prevents them from being deleted or copied. Directories and files will appear in NetWare NDIR scans if a user has the File Scan right.
Indexed	**I**		✓	Allows large files to be accessed quickly. Is useful for files 256KB (262,144 bytes) or larger. Only the maximum number of indexed files you designate at installation can actually use the turbo FAT indexes.
Normal	**N**	✓		Indicates no attributes have been set; corresponds with the public folder in the Macintosh environment.
Private	**P**	✓		Allows users to see the directory but not its subdirectories. This attribute does not prevent users from changing to the directory or its subdirectories if they know the correct path; corresponds to the private (gray) folder in the Macintosh environment.
Read Audit	**Ra**		✓	Not currently used by NetWare. Can be set, but has no effect.
Read Only/ Read Write	**Ro/Rw**		✓	Indicates whether a file can be modified. All files are automatically flagged Read Write when they are created and can be modified unless the Read Only attribute is set. Modify right required to remove the Ro attribute.
Shareable	**S**		✓	Allows several users to access a file simultaneously. Usually used in combination with the Read Only attribute.
System	**Sy**	✓	✓	Assign to system files and their directories. Hides these directories and files from DOS DIR scans and prevents them from being deleted or copied. Directories and files will appear in NetWare NDIR scans if a user has the File Scan right.
Transactional	**T**		✓	Activates TTS (**T**ransactional **T**racking **S**ystem). Prevents data corruption by ensuring all or no changes are made to files being modified. Especially helpful for database files.
Write Audit	**Wa**		✓	Not currently used by NetWare. Can be set, but has no effect.

NetWare utilities display the initial letters of these attributes between brackets. By convention, attributes that have not been assigned are indicated by dashes or blank spaces.

Use directory and file attributes to increase security in areas where many users have access to files. For example, NetWare utilities are flagged so that even the SUPERVISOR cannot accidentally delete them without removing flags.

- All NetWare files in SYS:SYSTEM, SYS:PUBLIC, and SYS:LOGIN are automatically flagged Ro and S.
- The bindery files are automatically flagged Sy, H, and T.
- Only FILER can be used to set archive and execute-only attributes.

To change or display file attributes, see FILER, FLAG, NDIR, and "Organizing and accessing files" in *Using the Network*.

To change or display directory attributes, see FILER, FLAGDIR, NDIR, and "Organizing and accessing files" in *Using the Network*.

Related utilities: FILER, FLAG, FLAGDIR, GRANT, REMOVE, REVOKE, RIGHTS, SYSCON, and WHOAMI /R in *Using the Network*.

Security equivalence

A security equivalence allows one user to have the same rights as another. Use security equivalence when you need to give a user temporary access to the same information or rights as another user. By using a security equivalence, you avoid having to review the whole directory structure and determine which rights need to be assigned in which directories.

SUPERVISOR can make any user security equivalent to another user or group, but Workgroup Managers and User Account Managers can assign security equivalences only within the pool of users and groups they manage. In networks containing confidential data that only selected users have access to, take care that you do not inadvertently give a user access to restricted information. Be aware that during the period the security equivalence is in effect, a user who is security equivalent to another user has all rights to that other user's home directory. Making a user security equivalent to a group would not have this disadvantage.

Be particularly cautious in making any user security equivalent to SUPERVISOR. Instead, delegate responsibilities to managers and operators.

See also **User; User Account Manager; Workgroup Manager;** and SYSCON and "Managing users and groups" in *Using the Network*.

Semaphore

Coordinates activities of both programs and processes to prevent data corruption in multiprocess environments. Semaphores with byte-value 0 allow a file to be shared. Byte-value 1 locks the file while in use, thereby preventing another user from accessing or altering an old file.

See also **File locking.**

Serial communication

NetWare uses the RS-232 serial communications standard to send information to serial printers, remote workstations, remote routers, and asynchronous communication servers. This standard, developed by the Electronic Industries Association (EIA), enhances the delivery of information from one system to another. A system can be any device or group of devices that can handle and process the data received. For example, a printer can be thought of as a system that transforms the binary data it receives from the computer into printed text. The RS-232 standard uses several parameters that must match on both systems in order for valid information to be transferred. These parameters include baud rate, character length, parity, stop bit, and XON/XOFF.

Baud rate is the signal modulation rate, or the speed at which a signal changes. Since most modems or serial printers attached to personal computers send only one bit per signaling event, baud can be thought of as bits per second; however, higher-speed modems may transfer several bits per signal change. Typical baud rates are 300, 1200, 2400, 4800, and 9600. The higher the number, the greater the number of signal changes and, therefore, the faster the transmission.

Character length specifies the number of bits used to form a character. The standard ASCII character set (including letters, numbers, and punctuation) consists of 128 characters and requires a character length of 7 bits for transmissions. Extended character sets (containing line drawings or the foreign characters used in IBM's extended character set) contain an additional 128 characters and require a character length of 8 bits. Parity error checking can only be used with character lengths of 7 bits.

Parity is a method of checking for errors in transmitted data. You can set parity to odd or even, or not use parity at all. When the character length is set to 8, parity checking cannot be done because there are no "spare" bits in the byte. When the character length is 7, the eighth bit in each byte is set to 0 or 1 so that the sum of bits (0s and 1s) in the byte is odd or even (according to the parity setting). For example, refer to the following illustration.

7-bit character	With Parity bit (odd parity)	With Parity bit (even parity)
1000001 (A)	10000011	10000010
1000010 (C)	10000110	10000111
1011000 (X)	10110000	10110001
1011010 (Z)	10110101	10110100

When each character is received, its parity is checked again. If it is incorrect (because a bit was changed during transmission), the communications software determines that a transmission error has occurred and can request that the data be retransmitted.

Stop bit is a special signal that indicates the end of that character. Today's modems are fast enough that the stop bit is always set to one. Slower modems used to require two stop bits.

XON/XOFF is one of many methods used to prevent the sending system from transmitting data faster than the receiving system can accept the information.

Serial port

A port that allows data to be transmitted asynchronously, one bit at a time. On IBM PC-compatible computers, COM1 and COM2 are asynchronous serial ports.

Serialization

Each NetWare operating system has a unique serial number. If two NetWare operating systems with the same serial number co-exist on the same internetwork, each file server displays a copyright violation warning at the file server console and at each logged-in workstation.

If a software or hardware error is suspected, call 1 (800) LANSWER (1 (800) 526-7937). You may be charged for the technical support to correct the errors.

If criminal copyright violation is suspected, please contact Novell's Customer Satisfaction Department at 1 (800) 453-1267 (in the USA).

Server

See **File server;** the *NetWare Print Server* manual.

Server protocol

See **NCP services.**

Service protocol

See **NCP services.**

SFT (System Fault Tolerance)

Data duplication on multiple storage devices; if one storage device fails, the data is available from another device. There are several levels of hardware and software system fault tolerance; each level of redundancy (duplication) decreases the possibility of data loss.

See also **Data protection; Disk duplexing; Disk mirroring.**

Shareable attribute

See **Security (Attribute security).**

Shell

See **NetWare workstation files.**

SHELL.CFG file

See **Boot files; Communication protocols; NetWare workstation files.**

Short machine type

A four-letter (or less) name representing a workstation brand. The name is set in the SHELL.CFG file. The default is IBM.

LOGIN uses this name as the %SMACHINE variable. The name is also used to load the correct screen color overlay file for NetWare menu utilities. The letters used are arbitrarily chosen; for instance, you could set the short machine type to CMPQ (`short machine type=cmpq`) in the SHELL.CFG file for an AT&T workstation that should use the black and white color palette (CMPQ$RUN.OVL).

See also **Color palette; Login script.**

Small Computer Systems Interface

See **SCSI.**

Software interrupt

See **Configuration option.**

Source routing

IBM's method of routing data across bridges (routers). NetWare source routing allows an IBM Token-Ring Network Bridge to forward NetWare packets (or frames).

IBM bridges can be configured as either single-route broadcast or all-routes broadcast. The default is single-route broadcast.

Single-route broadcasting means that only one designated single-route bridge will pass the packet and only one copy of the packet will arrive at its destination. Single-route broadcast bridges can transmit both single-route and all-routes packets.

All-routes broadcasting sends the packet across every possible route in the network, resulting in as many copies of the frame at the destination as there are all-routes broadcasting bridges in the network. All-routes broadcast bridges only pass all-routes broadcast packets.

To support IBM hardware and applications, Novell provides special source routing drivers: ROUTE.VP0 for the file server (the 0 in the extension directs the NetWare Operating System to load this VAP first) and ROUTE.COM for the workstation. (ROUTE.VP0 should be loaded first in most situations. If you use BACKUP.VAP, however, BACKUP.VAP must be run first. To load the two in the proper order, change BACKUP.VAP to BACKUP.VP0 and change ROUTE.VAP to ROUTE.VP1.) These drivers allow users running NetWare v2.2 to communicate across IBM Token-Ring Network Bridges. They also allow IBM applications that require source routing support to run unmodified on NetWare.

Parameters for ROUTE.VP0 determine which packets the file server broadcasts as all-routes packets and which as single-route packets. At the workstation, the ROUTE.COM file determines the type of packets the workstation broadcasts. It executes after IPX.COM and before the NetWare shell (NET*x*.COM).

See also **Router.**

Spool

To transfer data that was intended for a peripheral device (such as a printer) into temporary storage (such as a print queue). The data can then be transferred to the peripheral without delaying operating system or application operations.

In NetWare v2.2, CAPTURE is used to spool data to print queues. (Earlier versions of NetWare utilities and some applications use logical printer numbers (0-4) to specify network printers.) At the file server console, SPOOL creates, changes, or displays name mappings.

SPX (Sequenced Packet eXchange)

See **NetWare workstation files (IPX.COM).**

Station

See **Network station.**

Station address

See **Node number.**

Stop bit

See **Serial communication.**

Subdirectory

Any directory below another in the directory structure. For example, in SYS:ACCTS\RECEIVE, RECEIVE is a subdirectory of SYS:ACCTS.

See also **Directory structure.**

SUPERVISOR

See **User (SUPERVISOR).**

Surge protectors/suppressors

See **Power conditioning.**

Switch block

A set of switches mounted together to form a single component. In some file servers, a switch block is used to control system configuration data, such as type of monitor, amount of memory, and number of drives. Network boards often use switch blocks to set system addresses (such as station, base I/O, and base memory addresses).

Synchronous transmission

See **Serial communication.**

System attribute

See **Security (Attribute security).**

SYSTEM directory

A directory created automatically on the SYS volume during network installation. Copy the NetWare supervisor-only utilities into this directory during installation. This directory cannot be deleted.

System Fault Tolerance

See **SFT.**

System supervisor

See **User (SUPERVISOR).**

TTT

Tape backup unit

Typically, an external tape drive that backs up data from hard disks.

Terminating resistor

A grounding resistor placed at the end of a bus, line, or cable to prevent signals from being reflected or echoed. Sometimes shortened to terminator.

Termination

The last drive, controller, or HBA in any chain must be terminated.

See also **Hard disk; HBA; SCSI bus.**

Topology

The physical layout of network components (cables, stations, gateways, hubs, etc.). The three basic topologies include the following:

- Star network. Workstations are connected directly to a file server but not to each other.
- Ring network. The file server and workstations are cabled in a ring; a workstation's messages may have to pass through several other workstations before reaching the file server.
- Bus network. All workstations and the file server are connected to a central cable (called a trunk or bus).

Transaction Tracking System

See **TTS.**

Transactional attribute

See **Security (Attribute security); TTS.**

Trustee rights

See **Security (Rights security).**

TTS

The NetWare Transaction Tracking System (TTS) protects database applications from corruption by backing out incomplete transactions that result from a failure in a network component. When a transaction is backed out, data and index information in the database are returned to the state they were in before the transaction began.

TTS is a standard feature on NetWare v2.2 dedicated servers. This function can be turned on and off. Even if you don't plan to add a multi-user database to your file server, TTS is valuable because it protects the NetWare bindery and the queuing database files from corruption.

Why have TTS in the file server? Mainframe, minicomputer, and network database systems have offered transaction backout capability for some time. In most cases, however, this capability is implemented as part of the database application software and not as part of the operating system. NetWare TTS is implemented at the operating system level on the file server. This method provides two major advantages over application-level implementation.

- **Improved tracking.** Transaction tracking performance improves dramatically with TTS in the file server because transactions are tracked in the file server, where file writes are transacted; less data is transferred across the network; and all transactions benefit from the speed of NetWare's disk caching system.
- **Support for applications without backup capability.** When a database application without backout capability allocates a physical record lock to a database file or a logical record lock to an open database, the application "implies" that it is making a transaction. At this point, TTS begins tracking this implicit transaction so that the transaction can be backed out if a failure occurs.

  When a database application without backout capability releases physical or logical record locks, TTS infers that the application has completed a transaction. At this point, TTS will cease tracking the transaction.

Three kinds of database applications benefit from TTS:

- Applications that don't have transaction backout capability (implicit transactions)
- Applications that have built-in transaction backout capability (such as Btrieve)
- Applications that use explicit NetWare TTS calls to provide transaction backout capability (such as "begin," "abort," and "end")

TTS protection. A transaction on a network can be saved improperly in any of the following situations:

- Power to a server or a workstation is interrupted during a transaction.
- Server or workstation hardware fails during a transaction (for example, a parity error or a network board error might occur).
- A server or a workstation hangs (a software failure) during a transaction.
- A network transmission component (such as a hub, a repeater, or a cable) fails during a transaction.

TTS protects data from failure in all of these cases by making a copy of the original data before it is overwritten by new data. If a failure occurs during the transaction, TTS can back out the transaction and restore the original data.

- If the file server fails, TTS will back out the transaction when the file server comes up again.
- If a workstation or network transmission component fails, TTS will back out the transaction immediately.

TTS can protect against these types of failures for any type of application that issues record-locking calls and stores information in records, including traditional databases, some electronic mail applications, and some workgroup appointment schedulers. Files such as word processing files that are not organized into discrete records are not protected by TTS.

How TTS operates. TTS guarantees that all changes to a file are either wholly completed or not made at all. To track transactions on a given file with TTS, you must flag the file as transactional.

Note: A file that is flagged transactional cannot be deleted or renamed; a file cannot be flagged while it is open.

When a workstation begins a transaction in a database file, TTS follows four basic steps to maintain the integrity of the file:

1. TTS makes a copy of the original data so that the original data can be restored if the transaction fails. The copy is placed in a file external to the database file. This external file contains all transaction backout information; only the operating system uses it.

2. TTS writes the changed data to the database file after the copy of the original has been written to the backout file.

3. TTS repeats Steps 1 and 2 for additional transactions (a single transaction can consist of a sequence of changes).

4. When all changed data has been written to disk, TTS writes a record to the backout file, indicating that the transaction is complete. Completed transactions will not be backed out if the file server, workstation, or network transmission components fail.

Record-locking thresholds. Since some database applications leave one or more records locked at all times (usually for copy protection), TTS allows you to set a locking threshold in the workstation so that an implicit transaction is not unnecessarily tracked when the application is started and the first record lock occurs. Setting the locking threshold prevents having an entire database session tracked as a single transaction or having too many transactions per file update.

TTS handles special backout cases. In addition to handling routine backout tasks, TTS can back out file truncations or extensions and multiple changes to the same data area during a single transaction. TTS can also back out interrupted transaction backouts (if the file server fails in the middle of backing out transactions from a previous failure).

TTS also holds all workstation record locks until a transaction is completed. This prevents the disaster that would result from the following situation:

- The application in Workstation #1 releases a lock on a record before the transaction is completed (written to disk).
- Workstation #2 locks and changes the same record in file server cache memory (also before the first transaction is completed).
- Workstation #1 fails and Workstation #2 completes its transaction (it is written to disk).
- Because Workstation #1 failed, its transaction is backed out, in this case over the transaction that Workstation #2 completed.

If NetWare TTS did not hold workstation records locks until transaction completion, the database would not contain the correct information, since the latest transaction (from Workstation #2) would have been incorrectly overwritten with data that existed before the failed transaction (from Workstation #1).

See also **Cache memory.**

Related utilities: FCONSOLE; FILER; FLAG (see *Using the Network*).

Turbo FAT

See **FAT (Turbo FAT).**

UUU

Uninterruptible power supply

(UPS) See **Power conditioning.**

UPS (Uninterruptible Power Supply)

See **Power conditioning.**

UPS monitoring

UPS monitoring allows the file server to monitor an attached uninterruptible power supply (UPS).

A Novell-approved UPS should be attached to each file server in the network to provide backup power. (You can also attach a UPS to workstations without installing UPS monitoring hardware on the workstations.) When a power failure occurs, NetWare notifies users. After a timeout specified with SERVER.CFG and ROUTER.CFG, the server logs out any remaining users, closes any open files, and shuts itself down. See "Managing the file server" in *Using the Network.*

If you install a Novell-approved UPS, you must also install or set a board in the file server to monitor the UPS. (If you have a microchannel file server, the UPS is monitored through the mouse port and does not require a board.)

A board can function as a UPS monitor board if the board's mounting bracket has a stereo phone jack. The following boards can be used:

- An AT-compatible HBA or third-party equivalent
- Standalone UPS monitor board
- Software-serialized (SS) keycard, required in NetWare v2.11 and below

In case of a power failure, the following message appears:

```
Commercial power has failed.  Server <servername> is running on battery
power.  Server <servername> will stay up for <n> minutes.  Prepare users to
logout.
```

This message and other UPS system messages are explained in the "System messages" section of *Installing and Maintaining the Network.*

See also **Power conditioning.**

User

Any person allowed to work on the network. Each person must be assigned a user identity, or username. Once a username exists as an object in the file server bindery, the user can log in to the file server with that username and access the network. Although any number of users can be created, the number of users that can be logged in simultaneously depends on the capacity you have purchased with your NetWare v2.2 operating system.

You can simplify user access to file server resources (such as applications, printers and print queues, or directories) by creating groups on the file server and giving groups access to resources. Once a group is created, you can assign users to the groups; as members of the group, users automatically inherit the group's privileges.

System-created users and groups. Two usernames and a group already exist in the file server bindery when the file server is first installed:

- SUPERVISOR is the username for the network supervisor or system administrator.
- GUEST is the username for anyone who needs temporary and restricted access to the file server.
- EVERYONE is the group that includes all users.

SUPERVISOR has all rights in all directories. These rights cannot be revoked, nor can the user SUPERVISOR be deleted or renamed. Because the user SUPERVISOR initially has no corresponding password, the network supervisor can log in to the file server when setting up the network environment. SUPERVISOR is a user bindery object with ID Number 1.

For maximum security, we suggest the following:

- Set a supervisor password in SYSCON the first time you log in as SUPERVISOR. Change this password regularly and do not select an obvious password such as a spouse's name.
- Create a second username to use when you work on the network as a regular user. Log in as SUPERVISOR only when you have supervisor tasks to perform.
- Set up a "back door" to the system in one of two ways:

  1. Create a fictitious user with an unpredictable (but unforgettable) username and password and make that user security equivalent to SUPERVISOR.

2. Create a fictitious user with an unpredictable (but unforgettable) username and password; make this user the user account manager for both the fictitious user and SUPERVISOR.

Use caution in making anyone security equivalent to SUPERVISOR. Instead, delegate system administration responsibilities to MIS (Management Information System) staff or organization managers. Once the persons selected have been created as users on the file server, they can be designated as one of the following:

- Workgroup manager—an assistant supervisor with rights to create bindery objects (such as users and groups) and manage the user accounts. A workgroup manager (or any other user) can also be designated as a user account manager for existing users.
- User Account Manager—a user with rights to manage user accounts, but no rights to create new bindery objects, such as users and groups. Workgroup managers are automatically user account managers for users they create. Existing users can be assigned to a workgroup manager (or any other user) for account management.
- File server console operator—a file server supervisor with rights to use FCONSOLE.
- Print server operator—a print server supervisor with rights to manage the print server.
- Print queue operator—a printing supervisor with rights to create, manage, disable, and enable print queues.

See also **File server console operator; Printing; User Account Manager; Workgroup Manager.**

GUEST serves as a username for anyone who needs temporary and restricted access to the file server. The user GUEST is present in the bindery as a user-type bindery object when the file server is first brought up. GUEST has no password, but you can require a password for GUEST's account.

GUEST is automatically a member of the group EVERYONE, and all rights flow from membership in that group. See the section on EVERYONE below. If you change trustee rights for the group EVERYONE, the same changes will apply to the GUEST account.

The network supervisor should evaluate the security needs of the network and determine whether to retain GUEST and, if retained, what rights temporary users can exercise and what information they can access. If someone needs to access the file server for a definite period of time, you might prefer to create a user account that has an expiration date.

For maximum security, we suggest the following:

- Require a password for GUEST's account. Assign GUEST a password in SYSCON and change it frequently. Do not allow GUEST to change the password.
- Delete GUEST from the group EVERYONE and assign specific trustee rights to directories and files GUEST is permitted to use.
- Delete GUEST from the file server if you have no temporary users.

If you want GUEST to have more privileges, you can

- Assign GUEST temporary rights to specific directories and files
- Create a GUEST subdirectory in the HOME or USERS directory to provide personal work space for GUEST

EVERYONE is a system-created group that includes all users created on the file server. Since the group EVERYONE is already in the bindery as an object when the file server first comes up, users are automatically made members of the group. Whenever all users need the same rights, grant those rights to the group EVERYONE.

Membership in the group EVERYONE automatically provides all users with Create and Write rights in SYS:MAIL and Read and File scan rights in SYS:PUBLIC (and subdirectories). Users can create and send electronic mail (but not reopen the mail once it has been sent to another user's mailbox), run NetWare utilities, execute DOS commands, and access applications residing in the SYS:PUBLIC directory.

The network supervisor can delete any user from the group EVERYONE or change EVERYONE's trustee rights in any directory (including rights automatically granted by the system). However, we do not recommend removing EVERYONE's trustee rights in the SYS:PUBLIC and SYS:MAIL directories because users would not be able to access NetWare utilities, electronic mail, or print job configurations unless you reassign these rights to individual users or groups.

Although EVERYONE can be deleted from the file server, we do not recommend doing so. If the group is deleted and then re-created, users would have to be added to the group one at a time.

Other users and groups. When you set up the network environment, you can define

- **Regular network users**—the persons for whom you create usernames and user accounts
- **Groups**—collections of network users who share applications, perform similar tasks, or have similar needs for information

- **Managers and operators**—users to whom you assign certain supervisor rights and responsibilities for system administration

See **User account** for detailed information regarding regular network users, groups, managers, and operators.

Related utility: SYSCON (see *Using the Network*).

User account

Each user has a user account that is part of network security and controls the user environment. Some account features are assigned to each user automatically; some must be assigned; some are optional.

Usernames can be up to 47 characters long but, for efficiency, a username usually follows one of the following formats.

- **Given name** (for example, user JANE and user RICHARD)
- **Surname** (for example, user DOE and user SMITH)
- **Initials and surname** (for example, user JDOE and user RDSMITH)

You are less likely to have problems with duplicate names if you assign initials and surnames.

The username is also the login name and must be supplied when logging in. Record the user's full name for your own information.

You can view a list of existing users with SYSCON's "User Information" option. When you select a particular username from that list, you can also view the user's account features and restrictions.

Group membership. Users are automatically assigned to the group EVERYONE and inherit the rights assigned to the group EVERYONE. Other groups are created in SYSCON as empty sets and then users are assigned or added. Group members inherit the rights assigned to groups.

By selecting a particular username from SYSCON's list of users, you can view a list of "Groups Belonged To." You can also view a list of existing groups with SYSCON's "Group Information" option. When you select the name of a particular group from the "Group Information" list, you can view the group's "Member List."

Home or username directories (optional). The home or username directory serves as personal workspace. If you want each user to have a home or username directory, you should plan a parent directory (such as SYS:HOME or SYS:USERS) for these directories. For a large system, you may prefer to set aside a separate volume for username directories.

For ease in system administration, each user's home directory name should be the same as that user's username (for example, SYS:USER\JANE or SYS:HOME\RDSMITH).

If you grant all trustee rights to users in their own directories, users can control access to files in their directories. Users, however, cannot restrict SUPERVISOR, who has all rights to all directories.

Users can use create files and work on projects without allowing other users to have access to their work. Once the work is completed, the files can be copied to a work or project directory (group workspace) where other users have rights to access the information.

If you set the "Create home directory" option in SYSCON or create users with USERDEF, username directories in volume SYS are automatically created when you create users (unless you create and specify a parent directory for username directories). Trustee rights for these directories are also assigned automatically.

Trustee rights. If users need to access specific directories and files (other than those automatically assigned by the system), you must assign users trustee rights to these directories. You can view directory trustee rights for any user by selecting that username from the list of users under SYSCON's "User Information" option.

Security equivalences. Security equivalences allow users to exercise rights equivalent to those of another user. Assigning a security equivalence is convenient when you need to give a user access to the same information another user already has access to. In networks containing confidential data that only selected users have access to, take care that you do not inadvertently give a user access to restricted information. In addition, use caution in assigning supervisor equivalence. Delegate responsibilities to managers and operators instead. You can view security equivalences by selecting a username from the list of users under SYSCON's "User Information" option.

ID numbers. These are random, hexadecimal numbers assigned by the file server to each bindery object (including users).

As user SUPERVISOR, you can view an ID number for an existing user by selecting the user from SYSCON's list of existing users and then selecting the "Other Information" option.

Mailboxes. Each user is provided with a mailbox that is stored in the SYS:MAIL directory and contains user login scripts and print job configurations. When users are created, NetWare automatically creates a mailbox directory (named with the user's ID number) and assigns all rights except Access control to the directory. Even if you are not using electronic mail, don't delete SYS:MAIL or any of its subdirectories, because login scripts are also stored in this directory.

User login scripts. These configurable batch files customize the network environment for individual users by initializing environment variables, mapping drives, and executing other commands.

You can view a user's login script by selecting that user from SYSCON's list of existing users and then selecting the "Login Script" option. If users are allowed to change their own passwords, they are also automatically allowed to change their own login scripts.

Print job configurations. Each user can use printing defaults or you can create print job configurations in PRINTCON and copy them from one user to another. Print job configurations are stored in each user's mailbox directory in SYS:MAIL.

Account management. Accounts can be managed in several ways:

- By the SUPERVISOR. The SUPERVISOR can manage the accounts of all users.
- By a Workgroup Manager. Workgroup Managers can create users and manage accounts for any user they create.
- By a User Account Manager. The SUPERVISOR can assign existing users or Workgroup Managers as User Account Managers. User Account Managers cannot create users, but they can modify the accounts of users they are assigned to manage. More than one manager can manage a user account.

You can determine which user or group manages an existing user's account by selecting that user from SYSCON's list of existing users and then choosing the "Managers" option. If a user (or group) manages other user accounts, you can also view a list of managed users and groups from SYSCON's "User Information" option by selecting the manager's username and then selecting "Managed Users and Groups."

Login restrictions. Restrictions can be assigned at the account level to make it difficult for unauthorized users to access the file server. When login restrictions are not met, an account is disabled so that no one can log in to the file server under that username.

You can restrict logins in the following ways:

- **Account balance restrictions.** If you have installed Accounting to monitor or limit network resources, you can assign initial account balances for users and specify credit limits. When the account balance is depleted, the account is disabled.

  You can view the account balance for particular users by selecting that user from SYSCON's list of existing users and selecting "Account Balance." If you have not installed accounting, this option will not appear on the "User Information" menu.

- **Expiration restrictions.** You can specify an expiration date for a user account. The account expires at 12:01 a.m. the following day. Any attempt to log in after the account expires will disable the account. The default is no expiration date.

  You can view an account expiration date by selecting a user from SYSCON's list of existing users and selecting "Account Restrictions."

- **Password restrictions.** You can specify whether to require passwords. If you require passwords, you can also specify the minimum length of passwords (the default is five characters), how often the password must be changed (the default is every 40 days), whether the user can change the password (the default is Yes), and whether the password must be unique (the default is No). For a password to be unique, it must be different from the previous eight passwords used by the account. If you allow users to change passwords, you automatically allow them to edit their own login scripts.

  You can also specify the number of times a user can log in with an expired password (grace logins) or the number of incorrect login attempts (the default is six times). When either number is exceeded, the account is disabled.

  You can view password specifications by selecting a user from SYSCON's list of existing users and selecting "Account Restrictions."

  See also **Security (Login security).**

Disk space restrictions. If the "Limit Disk Space" parameter is set during installation, you can limit the maximum number of blocks available to each user by selecting a user from SYSCON's list of users and selecting "Account Restrictions."

Connection restrictions. You can limit the number of workstations (connections) a user can log in from concurrently.

You can view concurrent connection limitations for a user by selecting that user from SYSCON's list of existing users and selecting "Account Restrictions."

Time restrictions. You can restrict the hours during which users can log in. Times are specified in half-hour blocks. You can assign all users the same times, or you can restrict users individually.

If you assign individual time restrictions, you can view the time restrictions for a user by selecting the user from SYSCON's list of existing users and selecting "Time Restrictions."

Station restrictions. You can restrict the physical locations that a user can log in from by specifying the network and node addresses of the workstation the user is permitted to log in from.

Station restrictions cannot be set with system default restrictions; they must be assigned individually.

You can view the stations a user is limited to by selecting the user from SYSCON's list of existing users and selecting "Station Restrictions." If the "Allowed Login Addresses" box is empty, no station restrictions are in effect.

Utilities for creating users. You can create network users with SYSCON, MAKEUSER, USERDEF, and NWSETUP. No matter which utility you use to create users, you must use SYSCON to modify user accounts for existing users or to create groups.

SYSCON. You can create users individually with the "User Information" option. If you want to set defaults that apply to all users, set the "System Default Restrictions" form before creating users. All login restrictions except station restrictions can be set in this way and then modified individually for any user who has different needs. Any features of user accounts not created automatically or created by defaults must be individually created or assigned.

MAKEUSER. You can create several users by creating and processing a .USR script with MAKEUSER. A .USR script is a list of commands in a text file that specify how to create users and user account features (such as group memberships, passwords, and time restrictions).

You can create a .USR script by using the cut and paste features of a text editor or by typing the script in the MAKEUSER script box. All commands in the .USR script must be entered in a specific order.

USERDEF. You can also create several users with similar characteristics with USERDEF. Instead of creating a .USR script (as with MAKEUSER), you can use the USERDEF template to specify the same parameters. When you have entered all the usernames, USERDEF creates users by creating a temporary .USR script that MAKEUSER processes.

When users are created with the defaults provided in USERDEF, each is automatically provided a basic login script that includes essential drive mappings. The first search drive is mapped to SYS:PUBLIC and the second to the appropriate DOS directory. The first network drive is mapped to the user's default directory. Although these mappings make it possible to begin working on the network immediately, they are more appropriate for a system login script.

USERDEF also supplies new users with an initial password and the SUPERVISOR's print job configurations.

You can customize the way USERDEF creates new users by creating a custom template to set new default parameters or edit the basic login script.

Although new users created with USERDEF can begin work on the network immediately, we recommend that you use USERDEF only in two instances:

- If you must get large numbers of new users on the network quickly (use the default template).
- If you want to create users in batches, but do not want to plan MAKEUSER scripts (create a custom template).

NWSETUP. This utility creates users when the system is first brought up. In addition to creating users, you can specify initial passwords and the path for each user's home directory.

See also **Accounting; Groups; User Account Manager; Workgroup Manager** and "Managing users and groups" in *Using the Network*.

Related utility: SYSCON (see *Using the Network*).

User Account Manager

This user or group member is given the right to manage specified user and groups accounts. Existing users can be assigned to a User Account Manager, to a Workgroup Manager, or to any other user or group for account management. Workgroup Managers automatically become User Account Managers for users they create. Even though account management is delegated, user SUPERVISOR still has all rights to manage user accounts.

User Account Managers can

- Delete managed users and groups
- Assign a managed user to a managed group
- Assign a managed user as user account manager

User Account Managers can also modify any options in SYSCON's "User Information" submenu that don't require file rights, including

- Account Balance
- Account Restrictions
- Change Password

- Full Name
- Groups Belonged To (if the groups are managed groups)
- Login Script
- Managed Users and Groups
- Managers
- Security Equivalences
- Station Restrictions

User Account Managers must be assigned file rights in the directory structure before they can assign or modify

- Directory trustee rights
- Disk space restrictions

User Account Managers cannot

- Create users or groups
- Assign managed users to a group the manager does not manage
- Modify the login restrictions of their own accounts (unless they are also assigned management of their own accounts)

Why have User Account Managers? If you assign experienced users as User Account Managers, especially in a large system, they can handle routine tasks such as assigning users to new groups or changing drive mappings (in individual login scripts), account restrictions, account balances, and so on.

The User Account Manager can oversee the activities of a workgroup, but even if you do not organize workgroups, you can delegate management responsibilities to User Account Managers.

A user can be managed by more than one User Account Manager. If you assign users and groups to more than one manager, you will have a backup if one of the managers is not available.

See also **User; Workgroup Manager;** "Managing users and groups" in *Using the Network.*

Related utility: SYSCON (see *Using the Network*).

Utilities

NetWare utilities add functionality to the NetWare operating system.

File server maintenance utilities.

BINDFIX	Use BINDFIX to correct problems in the bindery files such as disruption to trustee rights.
COMPSURF	Use COMPSURF to perform a comprehensive surface analysis of any questionable disks and to prepare those disks for installation in a NetWare file server.
DISKSET	Use DISKSET only on an HBA that has not yet been configured. Unlike other boards, an HBA does not have jumpers or switches for changing configurations. DISKSET sets the configuration in the EEPROM.
VREPAIR	Use VREPAIR to correct minor hard disk problems on a volume without destroying its data.
ZTEST	Use ZTEST to ensure the integrity of track 0. ZTEST destroys any data on a hard disk.

File server console commands. These are part of the NetWare v2.2 file server operating system (NET$OS.EXE) or router operating system (ROUTER.EXE) and are executed at the file server or router console. They monitor and regulate resources. The following are console commands:

BROADCAST
CLEAR MESSAGE
CLEAR STATION
CONFIG
CONSOLE (DOS command for nondedicated computer)
DISABLE LOGIN
DISABLE TRANSACTION
DISK
DISMOUNT
DISPLAY SERVERS
DISPLAY NETWORKS
DOS (for nondedicated computer)
DOWN
ENABLE LOGIN
ENABLE TRANSACTION
MONITOR
MOUNT
NAME
OFF
PRINTER
PURGE
QUEUE
REMIRROR
RESET ROUTER
SEND
SET TIME
SPOOL
TIME
TRACK ON
TRACK OFF
UNMIRROR
UPS
VAP
VER
WATCHDOG

Workstation utilities. NetWare workstation utilities are designed to change the network after initial installation or to perform network tasks. The two types of workstation utilities include command line utilities and menu utilities. You can perform most tasks using either type of utility. Both types are documented alphabetically in the "Utilities" section of *Using the Network*.

Command line utilities are executed at the DOS prompt. You can use these utilities to manipulate rights and attributes, copy and print files, log in and out of file servers, view file server information, and map network drives. Once you are familiar with the command line utilities, you will find them faster to use than the menu utilities.

Rights/ Attributes	**Users**	**Server**
FLAG	ATTACH	ATOTAL
FLAGDIR	CASTOFF	BINDFIX
GRANT	CASTON	BINDREST
REMOVE	LOGIN	NVER
REVOKE	LOGOUT	PAUDIT
RIGHTS	SEND	SECURITY
TLIST	USERLIST	SETPASS
	WHOAMI	SLIST
		SMODE
Printing	**Directories/ Volumes**	SYSTIME
		VERSION
CAPTURE		WSUPDATE
PSC	CHKDIR	
PSTAT	CHKVOL	**Files**
NPRINT	LISTDIR	
	MAP	NCOPY
	RENDIR	NDIR
		PURGE

Menu utilities allow you to perform network tasks by choosing options from menus. You can complete some tasks such as creating users only with a menu utility. The utilities are designed so that some options are available only to you as SUPERVISOR or to users designated as supervisor-equivalent or as operators. Menu utilities make it easier to remember how to complete tasks by displaying options.

COLORPAL Modify the color schemes for NetWare menu utilities.

DSPACE Limit and view available disk space.

FCONSOLE Perform file server tasks from a workstation: view and alter file server status, view file and lock activity, view file server statistics, purge salvageable files, broadcast messages, and view detailed user connection information.

FILER	View and modify volume, directory, and file information. You can grant and revoke trustee rights in FILER, as well as assign and modify directory and file attributes.
HELP	View on-line information about NetWare.
MAKEUSER	Create large groups of users (especially useful if you regularly create and delete large groups of users).
MENU	Run a .MNU file that you create to run applications.
NBACKUP	Back up and restore data on file servers and local drives.
PCONSOLE	Set up print server and print queues, control network printing, and view information about network printing.
PRINTCON	Define your preferred print options and set them up as standard configurations. PRINTCON serves as a database for print configurations that can be used when you print files with CAPTURE, NPRINT, and PCONSOLE.
PRINTDEF	Set up a database of printer definitions. You can define a device driver for network printers, plotters, and other devices. You can also define the forms that the print devices will use.
SALVAGE	Recover the most recently deleted files.
SESSION	Perform a variety of network tasks. SESSION combines the functions of several command line utilities into a single menu utility and is intended primarily for network users.
SYSCON	Create users and groups, specify Workgroup and User Account Managers, and designate trustee rights.
USERDEF	Create templates to define and then create large groups of users. USERDEF works in conjunction with MAKEUSER.
VOLINFO	Check a file server's total and available kilobytes; check directory entries by volume.

VVV

Value-added server

A separate, specialized, dedicated process (such as a print server or a database server) that fulfills a specific function for network users.

See also **VAP.**

VAP (Value-Added Process)

A process that runs "on top" of the NetWare v2.2 network operating system (in much the same way a word processing or spreadsheet application runs on top of DOS). VAPs work with the network operating system to provide enhanced services without interfering with the network's normal operation. VAPs must be run on a NetWare v2.2 router or a NetWare v2.2 file server.

Volume

A volume is a physical amount of hard disk storage space. Its size is specified during installation or maintenance. NetWare v2.2 volumes are limited to 255MB and one hard disk, but one hard disk can contain several volumes. A NetWare volume is the highest level in the NetWare directory structure (on the same level as a DOS root directory). A NetWare file server supports up to 32 volumes.

NetWare volumes can be subdivided into directories by network supervisors or by users who have been assigned the appropriate rights.

The first default network volume, SYS, contains the SYSTEM, PUBLIC, LOGIN, and MAIL directories and cannot be renamed or deleted. Additional volumes must be defined initially with INSTALL. Changing a volume's size, name, etc., requires redefining the volume with INSTALL. Changing the number of volumes or a volume's size destroys all directory and file information. Therefore, make sure a reliable backup copy exists before redefining (reinitializing) volume information.

Several NetWare utilities—including MAP and VOLINFO—list a file server's volume names in one form or another. In addition, the DOS DIR command lists the volume name for the specified network drive (for example, "Volume in drive F is SYS"). This corresponds to the DOS volume label shown by the DOS DIR command for local disks (floppy diskettes or workstation hard disks). (A local disk can be given a volume label during formatting or with the DOS LABEL command.)

When a volume is used as part of a directory path, either in NetWare documentation or on the screen (for example, when running the MAP command), the volume name is followed by a colon (:), as in SYS:PUBLIC.

Related utilities: INSTALL (see *Installing and Maintaining the Network*).

See also **Directory structure; Volume definition table.**

Volume definition table

The volume definition table keeps track of volume information such as the volume name, the volume size, and where the volume is located on the network hard disk. Each NetWare volume contains a volume definition table in its NetWare partition.

See also **Volume.**

Volume, removable

See **Disk.**

Wait state

A period of time when the processor does nothing; it simply waits. A wait state is used to synchronize circuitry or devices operating at different speeds. For example, wait states used in memory access slow down the CPU so that all components seem to be running at the same speed.

Wait time

In a NetWare UPS system, the number of seconds the UPS will wait before signaling to the file server that the normal power supply is off. The file server then alerts attached workstations to log out.

See also **Down time; Power conditioning; UPS monitoring.**

WAN (Wide Area Network)

A computer network not confined to a single location. A WAN communication system is distinguished from a local area network (LAN) by its ability to communicate over longer distances.

Workgroup Manager

An assistant network supervisor with rights to create and delete bindery objects (such as users, groups, or print queues) and to manage user accounts. A Workgroup Manager has supervisory privileges over a part of the bindery. When several groups share a file server, Workgroup Managers can provide autonomous control over their own users and data.

Workgroup Managers supplement, but do not replace, the user SUPERVISOR. Workgroup Managers can manage only those users and groups they create or those assigned to them for account management (by designating a Workgroup Manager as the User Account Manager). SUPERVISOR retains absolute control over the network.

Workgroup Managers do not automatically acquire rights to the directory structure and file system. These rights must be granted by SUPERVISOR.

Workgroup managers can

- Create users and manage their accounts
- Delete users they have created
- Create groups and add users they manage

Workgroup managers must be assigned directory trustee rights before they can assign or modify

- Directory trustee rights
- Disk space restrictions

Workgroup managers cannot

- Create a user and make that user security equivalent to SUPERVISOR
- Create a Workgroup Manager
- Manage users or groups they have not created unless they have also been designated as the User Account Manager
- Assign any rights they have not been assigned by SUPERVISOR
- Modify the login restrictions of their own accounts (unless they are also assigned management of their own accounts)

Designating a Workgroup Manager. A Workgroup Manager may be either a user or a group.

User. First create the manager as a user with SYSCON's "User Information" option.

Group. First create the group with SYSCON's "Group Information" option. If you designate a group as Workgroup Manager, each member of the group will have Workgroup Manager privileges.

A Workgroup Manager is not a bindery object. Instead, a set property called MANAGERS is added to the SUPERVISOR object. Any object security equivalent to an object listed in the MANAGERS property set is considered a Workgroup Manager. The bindery uses the Workgroup Manager's ID number to indicate that the Workgroup Manager is the User Account Manager for the users a Workgroup Manager creates.

Workgroup Manager hierarchy. SUPERVISOR creates Workgroup Managers, and Workgroup Managers create and manage users. However, Workgroup Managers cannot create other Workgroup Managers. More complex hierarchical relationships can be created by controlling the level in the directory structure at which Workgroup Managers are given rights.

For maximum security, we suggest the following.

- Specify passwords in SYSCON for all Workgroup Managers' accounts.
- Require Workgroup Managers to create a second username to use when working on the network as regular network users. They should log in under the Workgroup Manager username only when performing management tasks.
- Use caution in making anyone security equivalent to a Workgroup Manager.

User Account Manager. When a workgroup is reorganized or a system is upgraded, existing users (and groups) can be assigned to a Workgroup Manager (or any other user or group) for account management. The user who manages a reassigned user, whether a Workgroup Manager or another user or group, is called a User Account Manager. If a group is assigned as User Account Manager, a user may have more than one manager, but you can also assign an account to be managed by one or more users.

As network supervisor, you can automatically assign users to workgroups when you create users if you first create usernames for Workgroup Managers and then designate these users as Workgroup Managers. Or you can create a group called MANAGERS, create the prospective members as users, and then assign them to the group.

Workgroup Manager rights. Assign each Workgroup Manager all rights in a volume or a directory. Next, log in using each Workgroup Manager username in turn, specify the parameters for user accounts, and then create the users for each workgroup. Each Workgroup Manager is automatically the User Account Manager for all users in the workgroup.

You can determine who manages a user's account by selecting that user from SYSCON's list of existing users and then choosing the "Managers" option. Although SUPERVISOR has all rights to create and delete users and modify user accounts, SUPERVISOR is not listed with "Managers."

By selecting the username of the Workgroup Manager or User Account Manager and then selecting "Managed Users and Groups," you can also view a list of managed users and groups with SYSCON's "User Information" option.

See also **User (SUPERVISOR); User Account Manager;** "Managing users and groups" in *Using the Network.*

Related utility: SYSCON (see *Using the Network).*

Workstation

A personal computer that is connected to a NetWare network and used to perform tasks through applications or utilities.

Workstation boot files

See **Boot files (workstation).**

Workstation shell

See **NetWare workstation files.**

Write Audit attribute

See **Security (Attribute security).**

Write right

See **Security (Rights security).**

XXX

XON/XOFF

See **Serial communication.**

ZZZ

ZTEST

An INSTALL utility that ensures the integrity of track 0. NetWare requires a flawless track 0 on every file server hard disk. INSTALL prompts you to run ZTEST for new hard disks.

ZTEST destroys all data on a hard disk, so be sure to back up any data you want to save.

Trademarks

Novell, Inc. has made every effort to supply trademark information about company names, products, and services mentioned in this manual. Trademarks indicated below were derived from various sources.

3Com, 3Com EtherLink, and EtherLink Plus are trademarks of 3Com Corporation.
286A and 286B are trademarks of Novell, Inc.
Acer 910 and Acer 1100 are trademarks of Acer Corporation.
ADIC is a registered trademark of Advanced Digital Information Corporation.
AppleTalk is a registered trademark of Apple Computer, Inc.
ARCnet is a registered trademark of Datapoint Corporation.
AST products are trademarks of AST Research, Inc.
AT&T is a trademark of AT&T.
Btrieve is a registered trademark of Novell, Inc.
Citizen is a trademark of Citizen Watch Co., Ltd.
CItoh 310/315 and CItoh 600 are trademarks of CItoh Corporation.
COMPAQ is a registered trademark of Compaq Computer Corporation.
Corona is a trademark of Corona Data Systems, Inc.
DESQview is a trademark of Quarterdeck Office Systems, Inc.
Diablo is a trademark of Diablo Systems, Inc.
Epson is a registered trademark of Epson America, Inc.
Gemini is a registered trademark of Star Micronics America, Inc.
GigaTrend is a registered trademark of GigaTrend, Inc.
Hayes is a registered trademark of Hayes Microcomputer Products, Inc.
Hewlett-Packard is a trademark of Hewlett-Packard Company.
Hot Fix is a trademark of Novell, Inc.
HP LaserJet is a registered trademark of Hewlett-Packard Company.
Hyundai SUPER-286 and Hyundai SUPER-286C are trademarks of Hyundai Corporation.
IBM is a registered trademark of International Business Machines Corporation.
IBM PC AT/XT are trademarks of International Business Machines Corporation.
IBM PC Network is a registered trademark of International Business Machines Corporation.
IBM Personal System/2 is a registered trademark of International Business Machines Corporation.
IBM ProPrinter is a registered trademark of International Business Machines Corporation.
ImageWriter is a registered trademark of Apple Computer, Inc.
Internetwork Packet Exchange (IPX) is a trademark of Novell, Inc.
LANSchool is a trademark of LANSystems, Inc.
LANSWER is a trademark of Novell, Inc.
Laserline is a registered trademark of Oki America, Inc.
LaserWriter is a registered trademark of Apple Computer, Inc.
Micro Channel is a trademark of International Business Machines Corporation.
Microline is a registered trademark of Oki America, Inc.
Mitsubishi MP286 and Mitsubishi MP386 are trademarks of Mitsubishi Corporation.
MS-DOS is a trademark of Microsoft Corporation.
NCR Model 8 is a trademark of National Cash Register Co.
NEC APC IV PowerMate 1 and NEC APC IV PowerMate 2 are trademarks of Nippon Electronics Corporation.
NetWare and Novell are registered trademarks of Novell, Inc.
NetWire is a trademark of Novell, Inc.
Novell RX-Net is a trademark of Novell, Inc.
Okidata is a registered trademark of Oki America, Inc.
OS/2 is a registered trademark of International Business Machines Corporation.
Panasonic is a registered trademark of Matsushita Electric Industrial Company, Ltd.
PC-DOS is a trademark of International Business Machines Corporation.

Personal Computer AT and Personal Computer XT are trademarks of International Business Machines Corporation.
Personal System/2 is a trademark of International Business Machines Corporation.
Pinwriter is a registered trademark of NEC Corporation.
SFT is a trademark of Novell, Inc.
Spinwriter is a registered trademark of NEC Corporation.
Star is a registered trademark of Star Micronics America, Inc.
The Coordinator is a registered trademark of Action Technologies, Inc.
Token-Ring is a trademark of International Business Machines Corporation.
Toshiba is a registered trademark of Toshiba America, Inc.
TTI is a trademark of Transitional Technology, Inc.
TTS is a trademark of Novell, Inc.
UNIX is a trademark of AT&T Bell Laboratories.
VAX and VMS are registered trademarks of Digital Equipment Corporation.
Wangtek is a trademark of Wangtek, Inc.
Western Digital is a registered trademark of Western Digital Corporation.
WordPerfect is a trademark of WordPerfect Corporation.
WYSE is a registered trademark of Wyse Technology.
Zenith Z300 is a trademark of Zenith Corporation.

User comments

Novell manuals and Novell products

We at Novell would like to hear from you if you have comments about our manuals and products, or have suggestions for improving them. Please address responses to

Novell, Inc.
Technical Publications
122 East 1700 South MS C-24-1
Provo, UT 84606 USA

Please indicate the relevant chapters and page numbers and other pertinent information as requested below.

Product Name: **NetWare v2.2** Edition: **March 1991**

Manual Name: **Concepts**

Your Name: _____

Company Name: _____

Address: _____

_____

City: _____ State/Province: _____

Country: _____ Zip/Postal Code: _____

Phone Number: ( ) _____

FAX Number: ( ) _____

Comments or suggestions

_____

_____

_____

_____

_____

Index

Master index

The contents of this index include the following manual codes next to page numbers:

C- *Concepts*
I- *Installing and Maintaining the Network*
U- *Using the Network*

The "System messages" section of *Installing and Maintaining the Network* is not indexed. It is an alphabetical listing itself.

login script command U-86. *See also* Login script
3C503 network board cabling, specifying DIX or BNC U-42. *See also* Cabling
8086 processor
  performance in real mode C-123
  in real-mode router C-130
8088 processor, in real-mode router C-130
80286 processor
  performance in protected mode C-120
  performance in real mode C-123
  used in routers C-130, C-131
80386 processor
  performance in real mode C-123
  used in routers C-130, C-131
80486 processor
  performance in real mode C-123
  used in routers C-130, C-131

A

Abend, defined C-1, I-212. *See also* "System messages" in *Installing and Maintaining the Network*
Access Control right, defined C-136. *See also* Security
Account, user. *See* User account
Account balance. *See also* Accounting; Login restrictions; User account
  defined C-2, C-159
  restrictions, defined C-76, C-159
  setting U-123
Account management, defined C-159
Account restrictions, defined C-135, C-159
Accounting. *See also* Login restrictions; User account
  account balance, default, setting U-439
  account balance, user, setting U-149, U-442
  charge rates, assigning U-147, U-437
  charge rates, calculating U-146
  defined C-1, U-145
  display summary of usage U-251
  installing U-145
  options C-2
  planning U-119
  records, viewing U-388
  removing U-150
  servers, authorizing to charge U-145
  servers, defined C-3
Active hub *See also* Hub; Passive hub
  defined C-4
  problems with I-250
Adapter, host bus (HBA)
  adding I-85
  choosing configuration option I-113
  configuring with DISKSET I-10
  Novell-approved I-10, I-14
  problems with I-236
  removing I-89
  setting and installing I-19
  setup program for I-40, I-85
  using NetWare Print Server with I-14
Adapter, problems with Token-Ring I-253
Add-on boards
  defined C-4, C-84, C-102
  installing I-11
Address
  base I/O, changing I-113, I-120
  base I/O, defined C-26
  base I/O, setting I-15
  base memory C-26
  controller C-28
  network, recording unique I-16
  in OS generation module I-34
  network, changing U-290
  network, defined C-96
  network, setting I-116
  node, changing U-290
  nondedicated DOS process C-100

Address *(continued)*
nondedicated network, changing I-115
nondedicated network, selecting I-12, I-61
Address, problems with
ARCnet boards I-250
Ethernet boards I-252
external hard disk I-235
file server I-233
internal hard disk I-234
multiple file servers I-244
routers I-244
Token-Ring boards I-253
workstations I-242, I-248, I-256
Advanced features, INSTALL I-65
All-routes broadcasting, defined C-145
Applications. *See also* Directory
creating directories for U-112
defined C-4
fake root, mapping U-113
files, assigning attributes for U-114
files, loading into network directories U-28
installing on the network U-113
memory required for I-16
not designed for network printing U-139
printing from U-138
printing from, with NetWare utilities U-139
Applications, problems with
access denied I-262, I-263
database contamination I-267
database too slow I-270
DOS utility I-268
file and record locks I-266
file not found I-264
general failure I-269
installation I-258
multiple users I-263
reading files I-262
trustee rights I-271
version I-260
Archive. *See* Backup; Restore
Archive Needed attribute C-140. *See also* Security
ARCnet board, problems with I-233, I-250
ASCII text file extensions, defined C-63
Asian character set, byte requirements C-86
Asynchronous transmission C-142
ATOTAL utility. *See also* Utilities
role in accounting C-3
using U-251
ATTACH login script command. *See also* Login script
defined C-5
using U-75
ATTACH utility U-252. *See also* Utilities
Attribute security C-139. *See also* Security
Attributes, directory. *See also* Security
listed C-140
planning C-139, U-114
setting U-333
viewing U-328
Attributes, file. *See also* Security
assign to network applications U-114
indexed, assigning I-22
indexed, changing I-94
listed C-140
planning C-139, U-114
setting U-331
setting for several U-329
transactional, assigning I-24
transactional, changing I-131
viewing U-330
Auto endcap, specifying C-119
AUTOEXEC.BAT file, creating
dedicated file server U-6
nondedicated file server U-7
ODI workstation U-41, U-42
remote reset U-31
workstation U-30
AUTOEXEC.BAT file, defined
all types defined C-10
DOS partition C-107
expanded memory C-91
extended memory C-92
multiple C-126
nondedicated file server C-107
remote reset C-126
AUTOEXEC.SYS file
creating U-11, U-440
defined C-14, U-11
example U-12
modifying U-440
Automatic rollback, defined C-5

B

Backing out, defined C-150
Backout volume, TTS C-150, I-23, I-44, I-131
Backup
BACKUP VAP, requirements U-27
defined C-7, U-26
DOS device U-368

NBACKUP, requirements U-26
NBACKUP, using U-367
third-party programs, requirements U-27
Bad blocks
adding to bad block table U-463
listing U-280
Banner page information, setting C-119
Base I/O address. *See also* Address
defined C-26
setting I-15, I-113, I-120
Base memory address, defined C-26. *See also* Address
Battery, monitoring UPS U-15
Baud rate, specifying for serial printer C-116, C-142
Bindery
backing up U-25
checked during file server boot U-9
defined C-8
maintenance U-24
repairing corrupt I-243, I-244, U-253
restoring a previous version U-255
Bindery objects
creating on file server U-28
defined C-9
setting maximum number of I-25, I-45, I-97
BINDFIX utility C-164, U-253, I-208. *See also* Utilities
BINDREST utility U-255. *See also* Utilities
BIOS, defined C-9
Block
bad, adding to bad block table U-463
bad, listing U-280
defined C-9, C-61
BNC cabling, specifying U-42
Board. *See* Controller board; Network board
Boot disk, file server
creating for a dedicated server U-6
creating for a nondedicated server U-7
Boot disk, router
creating dedicated U-63
creating nondedicated U-64
Boot diskette, workstation. *See also* Remote reset
copying files onto I-56
creating U-27, U-29
DOS ODI, creating U-42
DOS ODI, creating master U-40
preparing I-53
Boot failure I-238
Boot files
checking version of I-248
corrupted, fix I-254
dedicated file server C-13
DOS workstation C-10
nondedicated file server C-14
nondedicated routers C-15
ODI workstation C-12
Boot record, defined C-15
Boot status, partition I-26, I-46, I-123
BOOTCONF.SYS file
creating U-33
defined C-126
role in remote boot C-125
Booting. *See also* Remote reset
file server U-8, U-30
router U-30, U-65
BREAK login script command U-77. *See also* Login script
Bridge. *See* Router
BROADCAST utility U-256. *See also* Utilities
Buffer. *See* Cache buffer; Communication buffer
Bus
defined C-15
host. *See* Host bus adapter (HBA)
topology C-149. *See also* Cabling; Topologies

C

Cabling
BNC, specifying U-42
DIX, specifying U-42
Ethernet system defined C-58
network backbone C-101
routers C-128
topologies C-149
verifying connections U-273
Cabling, problems with
established system I-232
Ethernet boards I-251
external hard disk I-235
hubs I-250
interference I-247
internal hard disk I-234
internetwork I-244
MAUs I-253
new installation I-211, I-238
terminators I-233, I-251
Token-Ring boards I-253
workstations I-241, I-248, I-256

Cache buffer. *See also* Communication buffer
changing number of I-90
defined C-17
determining number of I-12, I-34
dirty, defined C-20
monitoring U-19
unavailable I-245
Cache memory, defined C-17
Caching
directory C-18, I-29, I-138
file C-18
statistics, viewing U-316
CAPTURE/ENDCAP utility. *See also* Printing
defined C-114, C-117
using U-258, U-313
CASTOFF utility U-262. *See also* Utilities
CASTON utility U-263. *See also* Utilities
Channel
defined C-21
disk, locating I-23, I-100
disk statistics, viewing U-318
DMA, configuring I-15, I-113
elevator seeking C-57
hard disk, locating I-17, I-105
number, configuring I-19, I-85
role in disk duplexing C-31, C-43
role in disk mirroring C-45
Channel 0, using with hard disks I-17, I-100, I-105
Character length, specifying for serial printer C-116, C-142
Charge rates, defined C-3. *See also* Accounting
Charging for services. *See* Accounting
CHKVOL utility U-264. *See also* Utilities
CLEAR MESSAGE utility U-265. *See also* Utilities
CLEAR STATION utility U-266. *See also* Utilities
CMOS RAM, defined C-22
CMPQ$RUN.OVL file, defined C-22
Cold boot loader
defined C-22
role in booting explained C-13, U-8
Color palette
application problems I-261
changing U-267, U-271
defined C-22
COLORPAL. *See also* Color palette
defined C-165
IBM$RUN.OVL file U-267
monitors, effect on U-270
using to modify color palette C-23, U-267
COM1 and COM2 ports, defined C-143
COMCHECK utility U-273. *See also* Utilities
Command format, defined C-24
Command line utilities, defined U-245, C-165. *See also* Utilities
Communication
network C-102
serial C-142
Communication, problems with
ARCnet board I-250
between file servers I-243
boot failure I-238
buffers, insufficient I-244, I-246, I-250
established systems I-212
Ethernet board I-251
file server I-245
new installation I-238
Token-Ring board I-253
workstation connection I-248
workstation to file server I-240, I-254
Communication buffer. *See also* Cache buffer; Packet receive buffer
changing U-290, I-90
defined C-15, C-24
determining number of I-12, I-34
insufficient I-244, I-246, I-250
monitoring for performance U-23
Communication protocols, defined C-24
COMPSURF utility I-39, U-275, C-164. *See also* Utilities
CompuServe C-95
Computer installation, problems with I-231
COMSPEC login script command U-78. *See also* Login script
Concurrent logins, restricting C-77
Conditionals in login scripts U-90. *See also* Login script
CONFIG utility U-288. *See also* Utilities
CONFIG.SYS file
creating for ODI U-41
explained C-10
requirements I-259
Configurable batch file C-77
Configuration options
base I/O address, changing I-113
base I/O address, setting I-15
defined C-25
disk driver, changing I-113
disk driver, selecting I-35
DMA, defined C-25

DMA channel, changing I-113
DMA channel, setting I-15
hardware, changing I-80, I-105
hardware, explained C-25
hardware, setting I-17
hardware, viewing U-288
interrupt (IRQ), changing I-113
interrupt (IRQ), setting I-15
LAN driver, changing U-290
network board, changing I-120
network board, changing temporarily U-43
network board, setting I-15, I-35
number, setting I-15
operating system, changing I-80
preventing conflicts C-26
workstation, setting I-53
Configuration options, conflicts with
Ethernet frame I-252
external hard disk I-235
IPX.COM I-241
network board I-243
operating system I-240
Connection
cabling failure I-209
information, viewing U-316, U-317
list, defined C-75
monitoring for activity U-469
number, defined C-27
restrictions, defined C-77, C-160
usage statistics, viewing U-317
verifying cable U-273
workstation failure I-209, I-248
Connectivity
defined C-27
on internetwork defined C-73
Console. *See also* File server console
clearing the screen U-387
defined C-27, U-250
nondedicated, switching to console mode U-289
nondedicated, switching to DOS mode U-304
Console commands. *See also* Utilities
adding to AUTOEXEC.SYS U-11
defined U-245
listed C-164
problems with I-231
Console operator
creating U-127
defined C-65, U-118
CONSOLE utility U-289. *See also* Utilities
Controller board, hard disk
address defined C-28
address, needed for DISKSET U-296
defined C-28
deleting in DISKSET U-299
number of, in hard disk channel U-296
setting, adding I-100
type, changing I-105
type, checking I-10
type, recording I-17
type of in DISKSET U-296
Controller speed, adjusting interleave factor C-73
Coprocessor. *See* Host bus adapter (HBA)
Copy, files U-380
Core printing, defined C-28
CPU, speed problems with I-245
Create right, defined C-136. *See also* Security
Cylinder, defined C-28

D

Data communication, handshaking, defined C-69
Data duplication. *See* Disk duplexing; Disk mirroring; SFT
Data files, loading into network directories U-28
Data protection C-29. *See also* SFT
Database, problems with
periodic slowdown I-270
when to index I-247, I-270
Date
directory created, viewing U-328
file, setting for several U-329
file, viewing or changing U-330
file server, setting U-427
file server, viewing U-445, U-446
workstation, synchronizing with file server U-445
DCB (Disk coprocessor board). *See* Disk coprocessor board (DCB); Host bus adapter (HBA)
DCONFIG utility U-290. *See also* Utilities
Dedicated file server. *See* Dedicated mode; File server
Dedicated mode. *See also* Nondedicated mode
defined C-31
file server, booting C-65
file server, choosing I-122
protected, choosing I-59

Dedicated mode *(continued)*
real, choosing I-59
router C-31, C-129
Dedicated router. *See* Dedicated mode; Router
Default drive, defined C-32
Default login script. *See also* Login script
defined C-77
illustrated C-77
Default server, defined C-32
Delimiter, defined C-32
Device driver C-32. *See also* Disk driver
Device sharing, defined C-32
DGroup memory, improving performance with U-21
Direct memory access. *See* Configuration options
Directory
accessing C-37
accessing from login script C-53
application, creating U-112
application, planning C-38
attributes, defined 139
creating directory structure for U-27
creation date, setting for several U-329
creation date/time, viewing U-328
defined C-34
DOS, creating U-112
DOS, planning C-38
fake root, need for C-61
fake root level C-39
files, listing and sorting U-382
home, creating U-113, U-122
home, planning C-40
information, viewing U-328
LOGIN C-76
MAIL C-83
mapping fake root for applications U-113, U-359
owner, setting for several U-329
owner, viewing U-328
parent, defined C-34, C-107
projects, creating U-113
renaming U-414
root level C-37
system-created, listed U-111
trustees, listing U-328, U-330
trustees, removing U-413
work or project, defined C-36
Directory attributes, application problems I-259
Directory caching
capacity C-62
choosing I-138
defined C-18
failure of I-246
Directory entries
choosing number of I-29, I-49, I-136
defined C-33
improving file server performance U-21
Directory path
conventions C-35
current, displaying C-81
defined C-33, C-109
Directory security
creating rights on file server U-28
Maximum Rights Mask C-136
planning C-133, U-115
Directory structure
creating U-111
defined C-34, C-37
illustrated I-73
planning C-34
problems with application use I-259
problems with file use I-264
Directory table
block, defined C-42
corruption in I-237
defined C-42
Disable, defined C-42
DISABLE LOGIN utility U-291. *See also* Utilities
DISABLE TRANSACTIONS utility U-292. *See also* Utilities
Disk
channel statistics, viewing U-318
defined C-42
duplexing I-25, I-47, I-110
external, configuring the HBA's EEPROM U-296
FORMAT/S I-53
formatting U-275
formatting, explained C-44
maintenance, suggested U-18
mappings, viewing U-318
mirroring I-25, I-47, I-110
NetWare-ready I-40, I-81, I-129
number I-28, I-111
repairing U-463
partition, defined C-107
primary I-25
primary, changing status of I-110
secondary I-25
secondary, changing status of I-47, I-110
statistics, viewing U-319
status, viewing U-293
storage, planning I-16
Disk allocation block, defined C-61

Disk controller
configuration, changing U-290
defined C-43
terminating C-69
Disk coprocessor board (DCB). *See also* Host bus adapter (HBA)
specifying I/O address in SERVER.CFG file U-14
specifying type in SERVER.CFG file U-13
Disk driver. *See also* LAN driver
defined C-43
problems with external I-235
problems with internal I-234
verifying I-15
Disk duplexing
defined C-31, C-43
logical disk size I-47
restore duplexing U-412
turn off mirroring/duplexing U-451
Disk interface board, defined C-44
Disk mirroring
changing I-110
defined C-31, C-45
information, viewing U-318
logical disk size I-47
restore mirroring U-412
turn off mirroring/duplexing U-451
Disk size, logical
changing I-123
changing for Hot Fix I-98, I-99
checking, on newly-mirrored/duplexed disk I-110
duplexing I-47
mirroring I-25, I-46
Disk size, physical
changing I-123
changing for Hot Fix I-98
duplexing I-47
mirroring I-46
Disk space
limiting I-24, I-44, I-96
planning C-40
restrictions C-77, C-160. *See also* Login restrictions
user's, limiting U-444
Disk storage
charging for. *See* Accounting
user's, limiting U-309, U-442
volume space, viewing U-264
Disk subsystem, defined C-46
DISK utility U-293. *See also* Utilities
DISKCOPY I-7
Diskette
boot. *See* Boot disk, file server; Boot disk, router; Boot diskette, workstation
installation I-7
NetWare system I-7
Diskless workstation. *See* Remote reset
DISKSET
configuring HBAs with I-20, I-31, I-86
defined C-164
deleting disk/controller combination in U-299
modifying hard disk settings with I-104
recording new disk drive configuration with I-101, I-102
saving channel configuration in U-299
setup utilities I-3, I-40, I-129
specifying hard disk configuration with U-298
using, on EEPROM chip I-89
DISKSET utility U-296. *See also* Utilities
DISMOUNT utility U-301. *See also* Utilities
DISPLAY login script command U-79. *See also* Login script
DISPLAY NETWORKS utility U-302. *See also* Utilities
DISPLAY SERVERS utility U-303. *See also* Utilities
DIX cabling, specifying U-42
DMA (Direct memory access). *See* Configuration options
Documentation, third-party I-4
DOS
device, defined C-46
device, selecting for backup U-368
mode, switching to console mode U-289
partition, creating I-46, I-122
partition, defined C-107
prompt, defined C-120
root directory I-27, I-133
setup routine, defined C-47
switching to DOS mode from console mode U-304
utility U-304. *See also* Utilities
DOS, problems with
ODI protocol I-256
utilities won't work I-268
version required by application I-266
won't load I-209, I-254
DOS BREAK login script command U-80. *See also* Login script
DOS commands
DISKCOPY I-7
FORMAT I-53
FORMAT /S I-53

DOS directory
creating U-112
mapping search drive to C-79
planning C-38
DOS ODI. *See* ODI workstation
DOS SET login script command U-81. *See also* Login script
DOS VERIFY login script command U-83. *See also* Login script
DOS version
chart of shell files for C-94
defined C-47
mapping a drive to correct directory C-80
required for v2.2 I-31, I-83
DOSGEN utility. *See also* Utilities
using U-305
setting up remote boot with C-124
DOWN command U-245
Down time (UPS)
default U-15
defined C-47
DOWN utility U-308. *See also* Utilities
DOWNLOAD utility I-74
Drive
default, defined C-32
defined C-47
floppy C-37
letters, assigning C-49
logical C-47
physical C-47
DRIVE login script command U-84. *See also* Login script
Drive letter, mapping C-83
Drive mapping
changing or viewing U-359
creating or changing C-51, U-116, U-424
creating to fake root C-52
creating to SYS:PUBLIC C-121
defined C-48, C-83, U-116
deleting C-52
local C-48
network C-48
pointer to C-37
search, creating C-49, U-116, U-424
search mode, setting U-431
using in login scripts C-79
viewing C-50
Drive number, physical I-19, I-100
Driver, LAN I-35. *See also* Disk driver
Driver protocol files, types of C-95
Drives, problems with in applications I-261
DSK_DRV_XXX diskette I-37, I-102, I-106
DSPACE utility U-309. *See also* Utilities
DXMAID, using with ODI U-41
Dynamic memory, defined C-55

E

ECONFIG utility U-310. *See also* Utilities
Effective rights, defined C-137
Elevator seeking, defined C-57
Embedded SCSI, defined C-57, C-133
EMSNET*x*.COM file
adding parameters to SHELL.CFG U-45
use of with expanded memory C-91
using U-38
EMSNET*x*.EXE shell file
defined C-10, C-90
using with ODI U-40
Enable, defined C-57
ENABLE LOGIN utility U-311. *See also* Utilities
ENABLE TRANSACTIONS utility U-312. *See also* Utilities
Encrypted passwords, defined C-58, C-109
End cylinder field
changing I-124
setting I-26, I-46
ENDCAP utility U-313. *See also* Utilities
Erase right, defined C-136. *See also* Security
Error log file extensions, defined C-63
Error messages, in applications
"File not found" I-264
"General failure" I-269
Ethernet board, problems with I-251
Ethernet configuration, defined C-58
Ethernet LAN driver, configuring U-310
EVERYONE (group)
assigning trustee rights U-128
defined C-67, C-156, U-128
Executable file extensions, defined C-63
Execute Only attribute, defined C-140. *See also* Security
EXIT login script command U-85. *See also* Login script
Expanded memory shell. *See* EMSNET*x*.COM
Expiration, user account C-76, C-160. *See also* Login restrictions
Extended DOS partitions C-107
Extended memory shell. *See* XMSNET*x*.COM

EXTERNAL PROGRAM EXECUTION
login script command U-86. *See also* Login script
External router
defined C-129
using to connect networks C-73, C-99

F

Fake root directory
defined C-61
mapping U-98, U-359
mapping, for applications U-113
FAT (File Allocation Table)
defined C-61
errors in, correcting I-233, I-237
protecting against corruption C-29
Fault tolerance C-144. *See also* SFT
FCONSOLE utility C-165, U-314. *See also* Utilities
FDISPLAY login script command U-79. *See also* Login script
Ferro-resonant isolation transformer C-62, C-111. *See also* Power conditioning
File
application problems I-259
attributes, listed C-140
boot, on master workstation diskette C-83
caching, explained C-18
caching, problems with I-270
copying U-380
copying several U-329
currently in use, viewing U-321
dates, viewing or changing U-330
holding open U-342
I/O statistics, viewing U-322
listing U-382
locking C-124
maximum number of open I-22, I-43, I-93
maximum number of open indexed I-94
owner, viewing or changing U-330
problems reading from I-262, I-263
problems retrieving C-13
problems writing to I-266
purging, from server console U-409
purging, from workstation U-408
releasing hold on U-341
salvaging U-418
setting dates for several U-329
setting owner for several U-329
sharing, defined C-66, C-140
size, viewing or changing U-330
sorting U-382
status, viewing U-320
updating automatically U-472
viewing contents of U-329
File Allocation Table. *See* FAT
File attributes. *See also* Security
indexed I-22, I-94
list of C-140
planning U-115
transactional I-24, I-131
File extensions, defined C-63
File locking
defined C-64
problems with I-266, I-268, I-270, I-272
File Scan right C-136. *See also* Security
File server
attaching to U-252
backing up U-26
boot disk I-31
boot screen display U-8
booting, explained C-65
clearing screen U-387
clearing workstation from U-266
configuration I-42
connection information, viewing U-316
connection list C-75
connections, monitoring for activity U-469
current, changing in menu utilities U-247
dedicated, choosing I-11, I-12, I-34
default, defined C-32
defined C-65
definition module I-42, I-81
downing U-308
downing, explained C-65
hardware compatibility I-10
hardware configuration, viewing U-288
information, viewing U-438
installing I-31
listing from the server console U-303, U-430
maintenance utilities C-164
memory requirements I-11
mode, changing in INSTALL I-122
name, choosing I-21, I-43, I-92
name, displaying U-366
nondedicated, choosing I-11, I-12, I-34
nondedicated, switching to console mode U-289
nondedicated, switching to DOS mode U-304
performance, fine tuning U-16
performance, viewing U-314
power requirements I-11

File server *(continued)*
preferred, specifying U-36
restoring U-26
setup requirements I-10
statistics, viewing U-314, U-319
switching between console and DOS modes U-10
tracking screen, turn on U-449
tracking screen, turn off U-448
utilities, created by INSTALL I-39
utilities, relinking I-80
volume I-29, I-138
workstation connection, breaking C-76
File server, booting
AUTOEXEC.BAT file, creating for dedicated file server U-6
AUTOEXEC.BAT file, creating for nondedicated file server U-7
boot disk, creating for dedicated file server U-6
boot disk, creating for nondedicated file server U-7
procedure U-8
File server, date and time
setting U-427
synchronize workstations U-445
viewing U-445
viewing from server console U-446
File server, maintenance
disk U-18
memory U-18
File server, problems with
console commands I-232
hanging I-233, I-269
new installation I-211
slow speed I-245
slow statistics update I-247
File server console
operator, defined C-65
prompt, defined C-120
File server parameters
disk space, limit I-96
Hot Fix size, set I-98
maximum number of open files, specify I-93
maximum number of open index files, specify I-94
server name, change I-92
File service processes
changing U-21
checking I-243
insufficient I-246
FILER utility C-166, U-326. *See also* Utilities
FIRE PHASERS login script command U-88. *See also* Login script
FLAG utility C-141, U-331. *See also* Utilities
FLAGDIR utility. *See also* Utilities
changing attributes with C-141
using U-333
Floppy disk, defined C-42
Floppy diskette drive. *See* Drive
Form. *See also* Printing
changing number U-137
defined C-66
defining U-141
Format
DOS, defined C-44
hard disks U-275
NetWare, defined C-44
FORMAT/S I-53
Frame, defined C-66

G

Gateway, defined C-67
General failure, of applications I-269
GOTO login script command U-89. *See also* Login script
Grace logins, restricting for security C-135
GRANT utility U-335. *See also* Utilities
Groups
adding users to U-130
assigning rights to U-129
creating U-129
defined C-156, C-157
examples C-67
information, viewing U-438
planning U-128
trustee assignments, viewing U-438
GUEST (user), defined C-155, U-117

H

Handshaking, defined C-69
Hard disk. *See also* Disk
adding I-105
changing channels in DISKSET U-298
channels I-17
controller, terminating C-69
controller boards I-10
defined C-42, C-69
deleting in DISKSET U-299
external I-10

external and HBA, installing I-19
internal I-10, I-17
internal and controller, installing I-17
maintenance U-18
saving new channels in DISKSET U-299
setting controller board for new I-100
specifying type of in DISKSET U-296
Hard disk, problems with
contaminated database I-267
external, inaccessible I-235
Hot Fix disabled I-246
I/O error count I-246
internal, inaccessible I-234
space used up I-213
volumes won't mount I-236
Hard disk, setting and installing
external I-10, I-19, I-100, I-103
internal I-10, I-17, I-105, I-107
primary I-25, I-47, I-110
secondary I-25, I-47, I-110
Hardware. *See also* Configuration options; Network board; Cabling
configuration, recording and setting I-17, I-105
configuration, updating OS for new I-80
configuration, viewing U-288
configuration settings C-75
conflicts I-235, I-239
failure I-212, I-254
file server I-10
interrupt C-25
supported by v2.2 I-10
troubleshooting flow charts I-216
workstation I-51
Hashing, explained C-18
HBA. *See* Host bus adapter (HBA)
HELP utility. *See also* Utilities
printing from within U-340
using U-337
Hexadecimal C-71
Hidden attribute C-140. *See also* Security
HOLDOFF utility U-341. *See also* Utilities
HOLDON utility U-342. *See also* Utilities
Home directory
creating U-113, U-122
planning C-40
Host bus adapter (HBA)
adding I-85
configuring I-113
configuring, with DISKSET I-20
configuring for external hard disks U-296
defined C-71
Novell-approved I-10
problems with I-236
removing I-89
setting and installing I-19
setup program for I-40, I-85
specifying I/O address in SERVER.CFG file U-14
specifying type in SERVER.CFG file U-13
using NetWare Print Server with I-14
Hot Fix
defined C-30
redirection area C-30
size of I-46, I-47, I-98, I-123
Hub, defined C-72. *See also* Active hub; Passive hub

I

I/O address, base. *See also* Address
defined C-26
setting I-15, I-113, I-120
IBM computers, supported by v2.2 I-10
IBM$RUN.OVL file, defined C-22
ID numbers, user C-158
Identifier variables, login script commands C-81. *See also* Login script
IEEE 802.3 standard. *See also* Ethernet configuration
configuring Ethernet driver for U-310
defined C-58
IF...THEN login script command U-90. *See also* Login script
Image files. *See* Remote reset
INCLUDE login script command U-95. *See also* Login script
Indexed file attribute. *See also* Security
choosing I-22, I-94
defined C-140
Indexed files, maximum number of open I-22, I-44, I-94
Initializing
disks, using COMPSURF C-164, I-39, U-275
environmental variables, upon login C-77
LAN interface board, during booting U-9
network board, problems with I-233

INSTALL modules
file server definition I-42, I-81
linking and configuring I-39, I-80
operating system generation I-34, I-80
Track Zero Test (ZTEST) I-40, I-81
INSTALL program
flowchart I-79
parameters described I-65
Installation, problems with
applications I-258
file server I-211, I-231
INSTOVL I-39
INT2F.COM file, using with ODI U-41
Interleave, defined C-73
Internal bridge. *See* Internal router; Router
Internal router. *See also* Router
defined C-128
using to connect networks C-73, C-98
Internetwork
created with internal router C-128
using applications on I-267
Interrupt (IRQ)
defined C-25
setting I-15, I-113, I-120
Interrupt problems
applications I-260
ARCnet boards I-251
Ethernet boards I-252
Intruder detection/lockout U-441
IPX drivers, defined C-74, C-94
IPX.COM (Internetwork Packet Exchange) file
adding parameters to SHELL.CFG U-43
configuration conflict I-241, I-254
copying for Remote reset U-31, U-32
copying to a boot diskette U-30
created with WSGEN C-83
defined C-10, C-94
generating with WSGEN I-51, I-53, I-56
parameters U-36
IPX/SPX protocol
defined C-24, C-94
required for IPX drivers C-74
using in message packets C-85
IPXODI.COM file
defined C-12, C-95
using U-40
IRQ. *See* Configuration options; Interrupt
Isolation, of problems I-209
Isolation transformer, defined C-111. *See also* Power conditioning

J

Jumper block, defined C-75
Jumper pins, defined C-75
JUMPERS utility U-343. *See also* Utilities

K

Keycard, SS
specifying I/O address in SERVER.CFG file U-14
specifying type number in SERVER.CFG file U-13

L

LAN driver
addresses, defined C-87
configuration, changing U-290
configuring I-15, I-35, I-113, I-117
defined C-95
Ethernet, configuring U-310
files, using with ODI U-40
setting U-343
LAN interface board, initialized during file server boot U-9
LAN Support utility (LANSUP.COM file)
missing I-253
using with ODI U-41
LAN_DRV_XXX diskette I-7, I-32, I-35, I-37, I-117
Limits, disk space I-24, I-96
Line-surge suppressor, defined C-110. *See also* Power conditioning
Linking and configuring module I-39, I-80
LISTDIR utility U-347. *See also* Utilities
Local drive mapping, defined C-48
Local router, defined C-129. *See also* Router
Lockout (intruder detection) U-441
Locks
logical, viewing U-323
physical, viewing U-324
setting level of, for TTS U-429
Log in. *See also* Password
attaching to additional servers U-252
attaching to preferred server U-36
disabling U-291
enabling U-311
to file server U-348
process defined C-75

as SUPERVISOR U-69
tracking C-2
Log out
procedure U-350
process defined C-76
Logical disk size
changing I-123
checking, for mirrored disks I-110
of mirrored/duplexed disks I-25, I-47, I-98
Logical drive, defined C-47
LOGIN directory, defined C-76, U-112. *See also* System-created directories
Login
name C-157
process defined C-75
restrictions, defined C-135, C-159
security, defined C-134
Login script. *See also* Login script, system; Login script, user
commands, recommended C-81
conventions, defined C-79
creating for groups C-67
default, illustrated C-77
defined C-77
identifier variables, defined C-81
system, defined C-78
user, defined C-78
Login script, system
creating U-441
creating drive mappings in U-116
creating on file server U-27
defined U-70
modifying U-441
planning U-70
updating workstation files automatically in U-472
Login script, user
creating U-443
creating drive mappings in U-116
creating on file server U-27
defined U-70
modifying U-443
planning U-70
Login script commands
U-86
ATTACH U-75
BREAK U-77
COMSPEC U-78
DISPLAY U-79
DOS BREAK U-80
DOS SET U-81
DOS VERIFY U-83
DRIVE U-84
EXIT U-85
EXTERNAL PROGRAM EXECUTION U-86
FDISPLAY U-79
FIRE PHASERS U-88
GOTO U-89
identifier variables U-90
IF...THEN U-90
INCLUDE U-95
MACHINE NAME U-97
MAP U-98
PASSWORD_EXPIRES U-102
PAUSE U-103
PCCOMPATIBLE U-104
REMARK U-105
SHIFT U-106
WRITE U-107
LOGIN utility U-348. *See also* Utilities
LOGIN.BAK file C-78
LOGIN.EXE file C-77
LOGOUT utility U-350. *See also* Utilities
Long machine type
defined C-82
including in login script C-80
LPT1 or primary parallel port C-82, C-107
LSL.COM file. *See also* Parallel port
defined C-12, C-95
using with ODI U-40

M

MACHINE NAME login script command U-97. *See also* Login script
Machine type
defined C-82
specifying in login script C-79
Macintosh VAP, installing NetWare for I-25, I-45, I-109
MAIL directory, defined C-83, U-112. *See also* System-created directories
Mailbox, location of C-83, C-158
Maintenance
bindery U-24
cache buffers U-19
communication buffers U-23
DGroup memory U-21
dynamic memory pools U-19
file service processes U-21
introduction U-16
memory U-18
security U-24
volume U-25

MAKEUSER utility C-161, U-351. *See also* Utilities
Manager
  user account, creating U-126
  user account, defined U-118
  workgroup, creating U-127
  workgroup, defined U-118
MAP login script command U-98. *See also* Login script
Map or Mapping. *See also* Drive mappings
  defined C-83
  disk, viewing U-318
  local drive C-48
  network drive C-48
  printer, adding to AUTOEXEC.SYS U-11
  spooler, adding to AUTOEXEC.SYS U-11
  spooler, changing U-434
  spooler, creating U-134, U-137, U-406
  spooler, listing U-434
MAP utility U-359. *See also* Utilities
Master workstation diskette, defined C-10, C-83
MAU, problems with I-253
Maximum number
  bindery objects I-25, I-45, I-97
  open files I-22, I-43, I-93
  open indexed files I-22, I-44, I-94
  TTS transactions I-132
Maximum Rights Mask. *See also* Security
  defined C-136
  planning U-115
  setting for several directories U-329
  viewing U-328
Media, removable I-65. *See also* the "External Hard Disk Worksheet"
Megabyte field I-46, I-124
Memory
  board, defined C-84
  boards, installing add-on I-11
  cache buffers, monitoring for performance U-23
  DGroup, improving file server performance U-21
  dynamic, monitoring U-19
  expanded memory shell U-38
  extended memory shell U-38
  maintenance U-18
  page C-90
  pool, monitoring for maintenance U-19
Memory, problems with
  dynamic, peaked I-246
  failure of I-212, I-237
  workstation I-257
Memory requirements
  application I-16
  communication buffer I-12, I-90
  file server I-11
  for ODI workstation U-39
  router I-60
  workstation I-52
Menu
  changing color of U-267
  creating U-151
  example text file U-156
  executing U-157, U-361
Menu utilities, defined C-165. *See also* Utilities
MENU utility. *See also* Utilities
  changing color of U-267
  current server, changing U-247
  defined U-245
  effect of COLORPAL on C-23
  using U-247, U-361
Message
  allowing reception of U-263
  blocking reception of U-262
  clearing from server console U-265
  clearing from workstation U-256
  sending from server U-256
  sending from workstation U-423
Message packet, defined C-85
Message system, defined C-86
Mirroring status. *See also* Disk mirroring
  changing I-110
  disk number I-47, I-111
  primary disk I-25
  secondary disk I-25
Mode, dedicated
  defined C-31
  file server, choosing I-11, I-12, I-34, I-122, I-127
  file server, defined C-65
  protected and real, choosing I-59
  router C-31, I-59
Mode, nondedicated
  file server, choosing I-11, I-34, I-122, I-127
  file server, defined C-65
  file server boot files C-15
  router, choosing I-59
  router boot files C-15
  switching between console and DOS U-10

Modify right, defined C-136. *See also* Security
Modules, INSTALL
  file server definition I-42, I-81
  linking and configuring I-39, I-80
  operating system generation I-34, I-80
  Track Zero Test (ZTEST) I-40, I-81
Monitor. *See* Console; File server
MONITOR utility U-362. *See also* Utilities
MOUNT utility U-365. *See also* Utilities
Mouse port, specifying type in SERVER.CFG file U-13
Multiple file server network, defined C-87
Multiple-byte character, defined C-86
Multiserver network
  defined C-87, C-97, C-98
  using applications on I-267

N

Name
  file server, changing I-92
  file server, choosing I-21, I-43
  volume, changing I-135
  volume, determining I-28, I-48
Name Service, NetWare I-14
NAME utility U-366. *See also* Utilities
NBACKUP utility C-166, U-26, U-367. *See also* Utilities
NCOPY utility U-380. *See also* Utilities
NCP. *See* NetWare Core Protocol
NDIR utility U-382. *See also* Utilities
NE2.COM file C-12
NE2000.COM file C-12, C-95
NET.CFG file
  creating U-53
  defined C-13, U-52
  example U-53
NET$ACCT.DAT file C-2
NET$BIND.SYS file C-9
NET$BVAL.SYS file C-9
NET$DOS.SYS file C-124
NET$OS.EXE file
  defined C-13
  on a partition C-107
  using to link OS I-39
NET3.COM. *See* NETx.COM
NET4.COM. *See* NETx.COM
NETBIOS.EXE file
  adding parameters to SHELL.CFG U-49
  emulator C-89
  using with ODI U-41
  required by application I-260, I-264
NetWare
  diskettes, making working copies of I-7, I-31, I-32
  for Macintosh VAP, installing I-25, I-45, I-109
  operating system, defined C-92
  operating system, generating I-34, I-80
  partition C-107, I-26, I-45, I-46, I-122
  version, displaying U-460
NetWare Core Protocol C-89
NetWare Name Service I-14
NetWare Print Server, choosing I-14, I-35
NetWare-ready disks I-40, I-81, I-129
NetWire C-95
Network
  backbone C-101
  backing up U-26
  communication C-102
  defined C-96
  installing applications on U-113
  listing U-302
  number C-96
  printers, setting up I-14, I-125
  prompt C-120, U-9
  restoring U-26
  site, preparing I-10
  station C-102
  supervisor C-154
Network address. *See also* Address
  internetwork problems with I-244
  defined C-96
  changing I-116, U-250
  recording unique I-16, I-34
Network board
  configuration, changing temporarily U-43
  configuration, viewing U-288
  configuring for ODI workstation U-39
  defined C-102
  setting and installing I-15, I-116, U-343
Network board, problems with
  ARCnet I-250
  configurations I-243, I-254
  conflicts with multiple I-242
  Ethernet I-251
  faulty connections I-249, I-255
  initializing I-233
  installation I-231, I-238
  performance, slow I-248
  Token-Ring I-253
Network drive mapping, defined C-48
Network packets, boards receiving unequal number of I-247

Network printing. *See also* Printer; Printing
  choosing I-14, I-125
  print path, setting up C-116
NETx.COM file
  adding parameters to SHELL.CFG U-45
  configuration conflicts with I-254
  copying for Remote reset U-31, U-32
  copying to boot diskette U-30
  copying to ODI master boot diskette U-40
  defined C-10, C-93
  parameters U-35
  unloading U-35
  version U-35
Node address. *See also* Address
  configuring U-250
  defined C-102
Node address, conflicts with
  ARCnet boards I-250
  Ethernet boards I-252
  file server I-233
  internetwork I-244
  Token-Ring boards I-253
  workstations I-242, I-248, I-256
Noise, reducing C-111
Nondedicated DOS process address C-100. *See also* Address
Nondedicated mode. *See also* Dedicated mode
  defined 103
  file server, boot files C-14
  file server, choosing I-11, I-34, I-122, I-127
  file server, defined C-65
  router, boot files C-15
  router, choosing I-59
  router, defined C-129
Non-DOS device, selecting for backup U-368
NPRINT utility. *See also* Utilities
  defined C-118
  using U-384
Number, disk
  recording I-28
  setting I-111
Number of copies, specifying in print jobs C-119
Numeric notation system C-71
NVER utility U-386. *See also* Utilities
NWSETUP, creating users with C-162

O

Objects, bindery
  defined C-9
  setting maximum number of I-25, I-45, I-97
ODI (Open Data-link Interface) workstation
  boot diskette, creating U-42
  boot files C-12
  customizing configuration with NET.CFG U-52
  master boot diskette, creating U-40
  network board, installing U-39
  preparing U-38
  strategy, defined C-105
OFF utility U-387. *See also* Utilities
On-line documentation. *See* Help utility
Open Data-link Interface. *See* ODI workstation
Open files, maximum number of I-22, I-43, I-93
Operating system
  defined 92
  generation module I-34, I-80
  mode, file server I-12, I-34, I-127
  mode, router I-59, I-60
  NetWare, generating I-34, I-80
  parameters, planning I-12
  partitions, for other I-26, I-44, I-122
  version, displaying U-460
Operating system, problems with
  configuration I-240
  corrupted I-232
Operator, console C-157, U-127
Option 0
  disk controller I-37, I-53
  router I-63
OS/2
  prompt, defined C-120
  workstation files C-94
Overlay files, defined C-22

P

Packet
  defined C-85
  lost, troubleshooting U-24
  tracking screen, turning off U-448
  tracking screen, turning on U-449
Palettes, changing in menus U-267
Parallel port, LPT1 or primary C-82, C-107

Parallel printer
choosing functionality for I-125
recording information about I-14
Parameters, operating system I-12
Parent directory, defined C-34
Parity, specify for serial printer C-116, C-142
Partition
changing I-122
DOS, defined C-107
NetWare, defined C-107
planning I-26, I-46
Passive hub. *See also* Active hub; Hub
defined C-109
problems with I-250
Password
changing U-428
default restrictions, setting U-439
defined C-109
intruder detection/lockout, setting U-441
required at login C-75
restrictions, defined C-76, C-134, C-160. *See also* Login restrictions
restrictions, setting U-442
setting for SUPERVISOR U-70
PASSWORD_EXPIRES login script command U-102. *See also* Login script
Path, directory
defined C-109
displaying C-81
PAUDIT. *See also* Utilities
using with accounting C-3
utility U-388
PAUSE login script command U-103. *See also* Login script
PCCOMPATIBLE login script command U-104. *See also* Login script
PCONSOLE utility. *See also* Utilities
defined C-118, C-166
using U-389
PDF files, defined U-140
PHASERS (FIRE) login script command U-88. *See also* Login script
Physical disk size I-47, I-98
Physical drive, defined C-47
Physical isolation, troubleshooting I-209
Pinpointing problems I-210
Pointer. *See* Drive mapping
Port. *See also* Parallel port; Serial port
COM1 and COM2, defined C-143
hardware C-109
LPT1 C-82, C-107
software C-109
Power conditioning
defined C-109
ferro-resonant isolation transformer C-62, C-111
line surge suppressor C-110, I-52
uninterruptible power supply (UPS) C-111, I-11
Power failure, problems with C-109, I-212, I-237, I-267
Power requirements I-11, I-52, I-60
Primary disk
determining I-25, I-47
setting size of I-110
Print device. *See also* PRINTDEF
defining U-140
definitions C-119, U-140
functions, defining U-401
modes, defining U-403
Print driver C-114
Print forms
defining U-142
deleting U-142
editing U-142
specifying length and width U-142
Print function C-112
Print job configurations
advantages of U-139
copying U-144
creating U-143, U-394
default U-143
defined C-112
for users C-159
Print jobs (core printing)
changing priority U-410
defined C-113
deleting U-410
listing U-410
Print mode C-112
Print path C-116
Print queue (core printing)
assigning to printers U-133, U-137, U-406
checked during file server boot U-9
controlling U-389
creating C-116, U-132, U-136, U-137, U-406, U-410
creating a spooler assignment U-134, U-136
deleting U-137, U-406
destroying U-136, U-410
listing jobs in U-136, U-137, U-391, U-406, U-410
priority, changing U-137, U-406
spooler assignments, listing and changing U-434

Print queue (core printing) *(continued)*
status, viewing U-392
users, listing U-393
Print queue operator
creating U-132
defined C-116, U-118
listing U-393
Print server, choosing I-14, I-35, I-125. See also the *Print Server* manual
PRINTCON utility. *See also* Utilities
copying print job configurations U-144
creating print job configurations U-143
defined C-119, C-166
using U-394
PRINTCON.DAT file, copying U-144
PRINTDEF
defined C-119, C-166
defining forms U-141
defining print devices U-140, U-403
print device functions, defining U-401
using U-400
Printed circuit board C-75
Printer (core printing)
assigning queues to C-115
choosing, in installation I-14
configuration, viewing U-137, U-406
defining C-116, U-133
defining print devices for U-139, U-400
forms, defining U-141, U-403
logical, creating U-137, U-406
logical, destroying U-137, U-406
maintaining I-125
mappings, in AUTOEXEC.SYS U-11
polling period, setting U-137, U-406
problems with I-210
serial, configuring U-137, U-406
status, viewing U-137, U-406, U-407
Printer commands (core printing), listed U-135
PRINTER utility U-405. *See also* Utilities
Printing (core printing)
from applications C-117, U-138
changing a job's priority U-136
controlling U-389
customizing C-118, U-139
defining print devices U-139, U-400
deleting a job U-136
DGroup memory conflicts U-21
ending a capture U-313
explained C-28, C-112
files C-117, U-391
form number, changing U-137, U-406
form feed, inserting U-137, U-406
forms, defining U-141, U-403
from Help U-340
job configurations, creating U-394
jobs, listing in a queue U-136
printer-formatted files U-384
problems with shell file parameters C-13
process described C-113
redirecting a parallel port to a queue U-258
rewinding (reprinting) U-137, U-406
screen displays U-138
starting U-137, U-406
stopping U-137, U-406
text files U-138
top of form, marking U-137, U-406
Problem isolation I-210
Processes, file service U-21
Programming language file extensions C-63
Project directories, defined C-36
Prompt, defined C-120
Properties, bindery C-9
Property data set, bindery C-9
Protected mode, defined C-120. *See also* Real mode; Router
Protocol C-89
PSTAT utility U-407. *See also* Utilities
Public access, defined C-121
PUBLIC directory. *See also* System-created directories
application directories, creating in U-112
defined C-121, U-112
DOS directories, creating in U-112
Public files, defined C-121
PURGE command line utility U-408. *See also* Utilities
PURGE console command U-409. *See also* Utilities

Q

Queue
assigning to printer C-115
defined C-115
spooling to C-114
Queue management, defined C-115
Queue operator C-116, U-118. *See also* Printing
Queue users C-116
QUEUE utility U-410. *See also* Utilities

R

Read Audit attribute C-140. *See also* Security
Read Only attribute C-140. *See also* Security
Read right C-136. *See also* Security
Read Write attribute C-140. *See also* Security
Read-after-write verification, defined C-30
Real mode, defined C-123, C-129, C-131. *See also* Router
Record locks
  defined C-124
  logical, viewing U-323
  physical, viewing U-324
  problems with I-266, I-268, I-270, I-272
  setting level of, for TTS U-429
  thresholds C-152
Recursive copying C-124
Redirection area C-124. *See also* Hot Fix
Regulation, in power conditioning C-111. *See also* Power conditioning
REMARK login script command U-105. *See also* Login script
REMIRROR utility U-412. *See also* Utilities
Remote boot C-124, U-30
Remote connection, defined C-127
Remote reset
  remote boot files, creating U-305
  defined C-124, U-30
  multiple remote boot files, creating U-32, U-306
  single remote boot file, creating U-31, U-306
Remote router, defined C-129
Remote workstation, defined C-127
Removable volume
  dismounting U-301
  mounting U-365
REMOVE utility U-413. *See also* Utilities
RENDIR utility U-414. *See also* Utilities
Repeater lights, faulty I-252
Requirements
  DOS I-31, I-83
  file server I-10
  hardware I-10
  memory I-11, I-52
  power I-11, I-52
RESET ROUTER utility U-415. *See also* Utilities
Resource, defined C-127. *See also* Configuration options
Resources, problems with reducing I-212
Restore, using NBACKUP U-27, U-375
Restrictions, on users
  default disk space, limiting U-439
  default password restrictions, setting U-439
  default time restrictions, setting U-439
  intruder detection/lockout, setting U-441
  user disk space, limiting U-442, U-444
  user password restrictions, setting U-442
  user time restrictions, setting U-443
  volume space, limiting U-444
REVOKE utility U-416. *See also* Utilities
Rights. *See also* Security
  assigning U-120
  effective, viewing U-328, U-417
  listed C-136
  planning C-67, C-135, U-114
Rights, trustee
  assigning to groups C-67, U-129, U-335
  assigning to users U-124, U-335
  deleting U-416
  group, viewing U-438
  list of C-136
  user, viewing or changing U-444
RIGHTS utility U-417. *See also* Utilities
Ring network topology C-149. *See also* Cabling; Topologies
Root directory
  defined C-37, C-127
  mapping fake root U-113, U-359
ROUTE.COM file C-145, U-41
ROUTE.VP0 file, used in source routing C-128
ROUTEGEN I-59
Router
  adding VAPs to ROUTER.CFG U-65
  boot disk, creating nondedicated U-64
  boot disk, creating dedicated U-63
  booting U-65
  configuration, planning I-59
  dedicated protected-mode C-129, I-59
  dedicated real-mode C-129, I-59
  hardware compatibility I-59
  hardware configuration, viewing U-288
  IBM, using with ODI U-41
  internal vs. external C-128
  loading, VAPs U-65
  local vs. remote C-129
  memory requirements I-60
  nondedicated protected mode I-59
  power requirements I-60
  setting and installing I-61
  tracking screen, turning off U-448

Router *(continued)*
tracking screen, turning on U-449
using, to connect networks C-73
Router table
corrupt I-244
defined C-131
resetting U-415
ROUTER.CFG file
creating U-66
defined C-15
using U-67
ROUTER.EXE file
copying to boot diskette U-63
specifying VAP loading U-66
Routing buffer. *See* Communication buffer
RPLODI.COM file
defined C-12, C-131
using with ODI U-40

S

SALVAGE utility C-166, U-418. *See also* Utilities
Salvageable files C-133
Script. *See* Login script, system; Login script, user
SCSI host bus adapter, defined C-71, C-133
Search drive mappings
to application directory C-53
to batch files C-53
defined C-49, U-116
to DOS directory C-53
in login scripts U-116, U-424
in search mode, setting U-431
Search drive mapping, problems with
application use I-260
file use I-264
Secondary disk
determining I-25, I-47
setting size of I-110
Security. *See also* Directory security; User account restrictions C-135, C-160
assigning trustee rights to groups U-129
attribute security C-139
attributes, listed C-140
file server U-28
effective rights C-137
levels of C-133
login security C-134
maintenance U-24
Maximum Rights Mask C-136
planning C-133, U-114, U-120
trustee rights, listed C-136
user accounts, creating U-121
user accounts, planning U-117
verifying U-130, U-420
Security equivalence, defined C-141, C-158
SECURITY utility U-420. *See also* Utilities
Semaphores
defined C-142
in use, viewing U-324
information, viewing U-322
limits for applications I-263
SEND utility U-423. *See also* Utilities
Sequential test, running U-283
Serial communication, defined C-142
Serial number I-7, I-74
Serial port C-143
Serial printer
choosing I-125
setting and connecting I-14
Serialization, defined C-143
Server, file. *See* File server
Server, print. See the *Print Server* manual
SERVER.CFG file
checking U-16
creating U-12, U-440
defined C-14, U-12
function of U-12
modifying U-440
specifying VAP wait time in U-13
Service processes, monitoring U-21
Service protocol C-89
SESSION utility C-166, U-424. *See also* Utilities
SET TIME command U-9
SET TIME utility U-427. *See also* Utilities
SETPASS utility U-428. *See also* Utilities
SETTTS utility U-429. *See also* Utilities
Setup (or third-party equivalent) software
running I-17
running to add external hard disk I-101, I-106
SETUP routine, changing file server date and time with U-9
SFT (System Fault Tolerance) C-144
Shareable attribute C-140. *See also* Security
Shell descriptor area, in login scripts U-101

Shell files
defined C-93
updating automatically U-472
using for expanded and extended memory U-38
Shell files, workstation
copying for Remote reset U-31, U-32
copying to boot diskette U-30
ODI boot diskette, creating U-42
ODI master boot diskette, creating U-40
using parameters when loading U-35
version required U-30
SHELL.CFG file
conflicts with I-260
creating U-43
defined C-12, U-43
defining long machine type in C-82
replaced by NET.CFG U-52
setting DOS version in C-79
SHIFT login script command U-106. *See also* Login script
Short machine type
defined C-144
matching with overlay file C-22
Single server network C-97
Single-route broadcasting C-145
Size, volume I-27, I-48, I-133
SLIST utility U-430. *See also* Utilities
Small Computer Systems Interface (SCSI) C-71, C-133
SMODE utility U-431. *See also* Utilities
Software version, displaying U-386, U-461
Source routing C-145
SPOOL utility C-114, U-434. *See also* Utilities
Spooler mappings
adding to AUTOEXEC.SYS U-11
changing U-434
creating U-134, U-135, U-137, U-406
listing U-434
Spooling, defined C-114, C-145
SPX (Sequenced Packet eXchange) C-94
SS keycard
specifying I/O address in SERVER.CFG file U-14
specifying type number in SERVER.CFG file U-13
Standalone UPS monitor board
specifying I/O address in SERVER.CFG file U-14
specifying type in SERVER.CFG file U-13
Star network topology C-149. *See also* Cabling; Topologies
Station C-102
Station address. *See* Address
Station restrictions C-135, C-161. *See also* Login restrictions
Stop bit, specifying for serial printer C-116, C-143
Subdirectory
copying U-329
defined C-34, C-146
information, viewing U-347
listing U-347, U-382
sorting U-382
SUPERVISOR (user)
defined C-154, U-117
equivalent, defined U-118
logging in as U-69
setting password for U-70
Suppression, in power conditioning C-110
Surge protectors C-110
Switch block, defined C-146
Synchronous transmission C-142
SYS:LOGIN directory
defined C-36, C-76
system-created U-111
SYS:MAIL directory
defined C-36, C-83
system-created U-111
SYS:PUBLIC directory
defined C-36, C-121
system-created U-111
SYS:SYSTEM directory
defined C-36, C-147
system-created U-111
SYSCON utility. *See also* Utilities
creating groups with U-129
creating users with C-161
defined C-166
using U-435
System
defined, in serial communication C-142
directory structure, illustrated I-73
generation module I-34, I-80
login script, creating U-71
login script, defined C-78
System attribute C-140. *See also* Security
SYSTEM directory, defined C-36, C-147, U-112
System Fault Tolerance (SFT) C-144
System login script C-78. *See also* Login script
System supervisor C-154, U-117
System-created directories
LOGIN C-76
MAIL C-83

System-created directories *(continued)*
PUBLIC C-121
SYSTEM C-147
SYSTIME utility U-445. *See also* Utilities

T

Tables, in shell files C-93
Tape backup unit C-149
Terminating resistor C-149
Termination C-69, C-133
Time
default user restrictions, setting U-122
directory creation, viewing U-328
file server, setting U-427
file server, viewing U-445, U-446
problems keeping I-232
restrictions, defined C-77, C-135, C-160. *See also* Login restrictions
restrictions, setting U-443
used, charging for U-147
workstation and file server, synchronizing on U-445
TIME utility U-446. *See also* Utilities
Timeout count, specify in print jobs C-119
Tips, maintenance U-16
TLIST utility U-447. *See also* Utilities
Token-Ring board, problems with I-253
Token-Ring network, using with ODI U-41
Topologies C-149
TRACK OFF utility U-448. *See also* Utilities
TRACK ON utility U-449. *See also* Utilities
Track Zero Test (ZTEST)
module I-40, I-81
running U-283
Transaction Tracking System (TTS)
backout volume, selecting and recording I-23, I-44
backout volume, setting I-131
current transactions, viewing U-321
defined C-150
disabling U-292
enabling U-312
record locks, setting level of U-429
statistics, viewing U-325
Transaction Tracking System (TTS), problems with
backout volume full I-272
being disabled/shut down I-273
contaminated database I-268
deadlocked workstations I-272
Transactional file attribute C-140, I-24, I-131. *See also* Security
Transactions, determining number of active user I-24, I-44
Transients, power C-110
Transmission signal C-72, C-109
Troubleshooting
applications I-258
cabling, verify connections U-273
communication I-238
file servers I-230
getting outside help I-273
hard disks I-230
overview I-209
problem isolation I-210
record keeping suggestions U-17
TTS problems I-272
volumes I-230
workstations I-254
Troubleshooting utilities
BINDFIX I-208
COMCHECK I-208
DISK I-208
FCONSOLE I-208
VREPAIR I-208
Trunk network topology C-149. *See also* Cabling; Topologies
Trustee rights C-137, U-120, U-128. *See also* Rights; Security
Trustee rights, problems with
application use I-258, I-264, I-271
file access I-264
file reading I-262
writing to files I-266
Trustees. *See also* Security; User
assigning rights to C-67, C-137, U-335
listing U-328, U-447
removing U-413
TTS. *See* Transaction Tracking System (TTS)
Turbo FAT, defined C-62

U

Uninterruptible power supply. *See* UPS
UNMIRROR utility U-451. *See also* Utilities
UPLOAD utility I-72
UPS (uninterruptible power supply)
adding commands to SERVER.CFG U-13
attaching to file server C-153

defined C-111
monitoring C-153
specifying type of monitoring hardware U-13
status, viewing U-452
using I-11
UPS battery, monitoring U-15
UPS utility U-452. *See also* Utilities
User. *See also* Accounting; Login script, user; Security; Trustee rights; Trustees
account balance, setting U-149
adding, to groups U-130
creating U-351, U-453
defined C-154
deleting U-351
disk space, limiting for I-24, I-96
full name C-157
home directory, creating U-113, U-122
name C-157
information, viewing U-442, U-443, U-470
listing U-458
login restrictions defined C-76, C-159
rights, assigning to U-124
security, creating for U-28
trustee assignments, viewing or changing U-444
User account
creating U-121
defaults, planning U-118
defaults, setting U-121
defined C-157
planning U-117
User account manager
creating U-126
defined C-155, C-162, C-171, U-118
User ID number, defined C-83, C-158
User login script. *See also* Login script; Login script, user
creating U-72
defined C-78, C-159
planning U-70
USERDEF utility. *See also* Utilities
creating users with C-161
defined C-164
using U-453
USERLIST utility U-458. *See also* Utilities
Username C-157
USR file
creating U-351
editing U-358
Utilities
command line, listed C-165
console commands, listed C-164
defined C-164
file server maintenance, listed C-164
icons, explained U-245
menu, listed C-165
troubleshooting I-208
wildcards, using with U-246
workstation, defined C-165
Utilities, using
ATOTAL U-251
ATTACH U-252
BINDFIX U-253
BINDREST U-255
BROADCAST U-256
CAPTURE U-258
CASTOFF U-262
CASTON U-263
CHKVOL U-264
CLEAR MESSAGE U-265
CLEAR STATION U-266
COLORPAL U-267
COMCHECK U-273
COMPSURF U-275
CONFIG U-288
CONSOLE U-289
DCONFIG U-290
DISABLE LOGIN U-291
DISABLE TRANSACTIONS U-292
DISK U-293
DISKSET U-296
DISMOUNT U-301
DISPLAY NETWORKS U-302
DISPLAY SERVERS U-303
DOS U-304
DOSGEN U-305
DOWN U-308
DSPACE U-309
ECONFIG U-310
ENABLE LOGIN U-311
ENABLE TRANSACTIONS U-312
ENDCAP U-313
FCONSOLE U-314
FILER U-326
FLAG U-331
FLAGDIR U-333
format, explained U-246
GRANT U-335
HELP U-337
HOLDOFF U-341
HOLDON U-342
JUMPERS U-343
LISTDIR U-347
LOGIN U-348

Utilities, using *(continued)*
LOGOUT U-350
MAKEUSER U-351
MAP U-359
MENU U-361
MONITOR U-362
MOUNT U-365
NAME U-366
NBACKUP U-367
NCOPY U-380
NDIR U-382
NPRINT U-384
NVER U-386
OFF U-387
PAUDIT U-388
PCONSOLE U-389
PRINTCON U-394
PRINTDEF U-400
PRINTER U-405
PSTAT U-407
PURGE (command line) U-408
PURGE (console command) U-409
QUEUE U-410
REMIRROR U-412
REMOVE U-413
RENDIR U-414
RESET ROUTER U-415
REVOKE U-416
RIGHTS U-417
SALVAGE U-418
SECURITY U-420
SEND U-423
SESSION U-424
SET TIME U-427
SETPASS U-428
SETTTS U-429
SLIST U-430
SMODE U-431
SPOOL U-434
SYSCON U-435
SYSTIME U-445
TIME U-446
TLIST U-447
TRACK OFF U-448
TRACK ON U-449
UNMIRROR U-451
UPS U-452
USERDEF U-453
USERLIST U-458
VAP U-459
VER U-460
VERSION U-461
VOLINFO U-462
VREPAIR U-463
WATCHDOG U-469
WHOAMI U-470
WSUPDATE U-472

V

Value-added process. *See* VAP
Value-added server C-167
VAP (Value-added process)
adding commands to SERVER.CFG U-13
creating XBRIDGE.CFG file for U-66
defined C-167
DISK command for U-67
listing U-459
loading, on a router U-65
NetWare for Macintosh I-25, I-45, I-109
specifying, with ROUTER.CFG U-65
VAP utility U-459. *See also* Utilities
VER utility U-460. *See also* Utilities
Version
DOS I-31
DOS, used to boot file server I-83
NetWare operating system, displaying U-460
software, displaying U-386, U-461
VERSION utility U-461. *See also* Utilities
VOLINFO utility C-164, U-462. *See also* Utilities
Volume
attributes, setting U-333
backing out (TTS) I-23, I-44, I-131
caching I-29, I-48, I-138
defined C-34, 167
definition, planning I-27
definition table C-168
directory entries, choosing number of I-29, I-49, I-136
disk space on, limiting user's U-309, U-444
file server, setting up I-27, I-29, I-138
information, viewing U-462
maintenance, suggested U-25
mounted during file server boot U-8
naming I-28, I-48, I-135
problems mounting I-236
removable, dismounting U-301
removable, mounting U-365
size, setting I-27, I-48, I-133
space available on, viewing U-264
troubleshooting I-233
VREPAIR utility. *See also* Utilities
defined C-164
using U-463, I-39, I-208

W

Wait state C-169
Wait time (UPS)
  default U-15
  defined C-169
WAN (Wide area network) C-169
WATCHDOG utility U-469. *See also* Utilities
WHOAMI utility U-470. *See also* Utilities
Wide area network (WAN) C-169
Wildcard characters, using with utilities U-246
Work directories, defined C-36
Workgroup manager
  creating U-127
  defined C-155, C-169, U-118
Workstation. *See also* Connection; ODI workstation
  activity, viewing U-362
  boot diskette, copying files onto I-56
  boot diskette, creating U-27, U-29
  boot diskette, preparing I-53
  boot files, defined C-10
  configuration I-51
  configuration files, creating U-27
  connections, monitoring for activity U-469
  defined C-172
  files, updating automatically U-472
  hardware compatibility I-51
  memory requirements I-52
  power requirements I-52
  removing, from file server U-266
  shell, defined C-5, C-93
Workstation, troubleshooting
  connection failure I-209, I-248
  file server not found I-254
  flow charts I-226
  hanging I-269, I-272
  insufficient memory I-257
  name conflict with application I-261
  new installation I-211
Workstation utilities, listed C-165
Write Audit attribute C-140. *See also* Security
WRITE login script command U-107. *See also* Login script
Write right C-136. *See also* Security
Writing problems, in files I-266
WSGEN
  using I-54
  workstation shell files created by C-93
WSUPDATE utility U-472. *See also* Utilities

X

XMSNET*x*.COM file
  defined C-9
  using U-38
  using with extended memory C-92
XMSNET*x*.EXE shell file
  defined C-91
  using with ODI U-40
XON/XOFF, specifying for serial printer C-116, C-143

Z

ZTEST (Track Zero Test)
  defined C-164, C-173
  module I-40, I-81
  using U-283

NOVELL, INC.

122 EAST
1700 SOUTH

PROVO, UTAH
84606

(801) 429-7000
(800) 453-1267

MADE IN
U.S.A.

101-001125-001

100-000266-001

NOVELL®